The human factor of cyber security: a multi – disciplinary approach and qualitative analysis of the occurrence of scientific insights in the field considering the insider threat

Leiden University

Faculty of Governance and Global Affairs

MSc Crisis and Security Management

Supervisor: S. Wittendorp

Second Reader: B. Schuurman

Thesis coordinator: Dr. J. Matthys

Author: Christian Koolen

Student number: s1724622

Word count: 83068

Word count excluding bibliography & attachments: 51875

Table of contents

Chapter 1: Introduction

1.1 The hacker threat?

A video demonstration of the global crowdsourced penetration testing organization Synack was featured all across the internet on the fifth of July 2017. The video [1] showed a Russian white hat hacker: an ethical hacker with no malicious intention, [2] in service of Synack hacking the laptop of a reporter. The purpose of the video, within the context of potential Russian meddling with American elections ,[3] and possibly even global influence ,[4] becomes apparent very quickly: to show that the threat to be hacked is out there, and especially the Russians are behind it. Upon further analysing the video however, it becomes apparent very quickly how staged the setup really is. First of all, the nationality of the hacker should not matter for the substance of the video, even more so because the hacker is a white hat in service of an international organization and not in service of a clandestine Russian group sinisterly plotting global Russian dominance. It is understandable that the Russian nationality is mentioned here, because as I mentioned before 'Russian hackers' are a perceived threat in most areas of the West and thus a click-bait title will ensure more people view the article and from a business perspective, act upon it, i.e. buying some form of protection against this perceived threat. The next and most important point is however the way in which the hacker actually gains access to the reporters' laptop. The article itself mentions the ease through which the hacker skips through all security measures and takes complete control of the laptop within minutes. A true doomsday scenario it would appear for anyone who wishes to never be hacked: if a known specialist can do this with such ease, will we ever be safe from those who are equally specialized but have more malicious intentions? Luckily, further analysis of the video shows that it was not skilful hacker display, but the reporter herself who was the major spill. The only reason the hacker ever gained remote access to the reporter's laptop, was because the reporter connected to and completely entrusted a Wi-Fi network she supposed belonged to her hotel, but instead belonged to the hacker.

1.2 The appeal to human factors

The above story exemplifies the major theme of this thesis: the human factor in cyber security. At first it might appear to be a strange combination, curious at least. What exactly do humans contribute to cyber security? But as we will delve deeper within the security realm we will find out that the human factor encompasses a lot of things and might actually be equally or even more important than all of the technical aspects combined. As of now, let us start off with the notion that cyber threats are expected to be a continuation and intensification of cyber-attacks and threats from previous years, alongside new challenges that come with the currently blurring lines of states, markets, businesses, civil society and cyber space. [5] With

[1] https://www.cnbc.com/2017/08/05/watch-this-russian-hacker-break-into-our-computer.html
[2] T. Caldwell, *Ethical hackers: putting on the white hat,* in Network Security 7 (2011), 10
[3] https://www.nytimes.com/news-event/russian-election-hacking
[4] http://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003 ; https://www.pri.org/stories/2017-12-14/russia-s-influence-middle-east-growing
[5] http://www.energi.com/news/2017/01/2017-cyber-risks-to-intensify-as-hackers-become-more-cunning-report/

this in the back of our minds, we can generally assume the nature of the largest threats. One of such is for example ransomware: [6] a virus that encrypts your files and either threatens to delete them or will restrict access unless paid for a key. This virus, mainly the 'Wannacry' variant, hit not only multiple organizations and businesses worldwide, but also targeted personal computers everywhere causing serious financial damage. [7] As of September 2018 another volatile version named "Gandcrab" is on the march, featuring not only the traditional ransomware design, but also actively adapting against security measures. [8] The design behind the virus is not new, however, dating back to far before 2016's popular variants 'Locky' and 'Samas', but also 2013's popular variants Xorist, CryptorBit and CryptoLocker, [9] restricting a user's access to their infected systems until a ransom was received to unlock their files. This has been a lucrative and ongoing business for quite some time. While many modern variants feature a message prompt that files have been encrypted and ransom is required, many of the 'old' variants relied on some sort of appeal upon authority, such as police, justice departments, secret services, even royalty to scare victims into actually transferring a required 'fee' to release them of hefty charges such as illegal pornographic images, illegitimate access to state secrets, or even illegally downloading music, video or distributing content. [10] What we can see here, is that a certain appeal to human factors is at work. There is for example no money being stolen in a clandestine undetectable way, but through a carefully crafted social matter money is extorted (depending on what kind of virus is at work naturally).

1.3 Exposure, profit, and manipulation

So interestingly enough, the nature of these viruses differ a lot from what is traditionally perceived as the harm that malware causes. Though there is a great variety of motivation for hackers, let us take profit in mind. It would appear to be more interesting to use keyloggers, worms, rootkits or Trojan horses to infect someone's system and access private or sensitive information from one's hard disk or CPU directly in a clandestine way to gain access to one's financial means and drain it for a large sum. [11] A traditional example would be gaining access to one's credit card information and then transferring the money from the victim to a private bank account. A more modern example would be a virus that secretly renders some of the CPU power towards mining cryptocurrency, not nearly enough to be noticeable, while spreading itself to others systems in the network or wide area, creating an almost undetectable bot net that generates revenue for the one who created it. Interestingly enough, the most successful virus that struck in 2017 was the global ransomware attack, where the perpetrator, in a way, exposed himself to his victims and tries to manipulate them through something that resembles social engineering. In conclusion, somehow it has become more lucrative to pressure people instead of solely technically hacking a system.

---

[6] https://www.nrc.nl/nieuws/2017/06/27/volg-hier-de-ontwikkelingen-rond-de-wereldwijde-randsomware-aanval-a1564740
[7] https://www.dearbytes.com/alerts/wannacry/
[8] https://www.acronis.com/en-us/articles/gandcrab/
[9] https://www.us-cert.gov/ncas/alerts/TA16-091A
[10] https://www.pchulplijn.nl/helpdesk/virus-verwijderen/politievirus/persoonlijke-computer-wordt-geblokkeerd
[11] https://www.quora.com/What-is-the-purpose-of-computer-viruses ; https://www.technibble.com/why-do-people-create-computer-viruses/

1.4 Can security keep up?

As the hackers themselves seem to shift from mostly technical hacking to extract information towards mostly influencing and manipulating humans in combination with hacking, can we also see this shift for those who either seek or provide security? Do businesses and organizations have to adapt towards the same shift? And if they do, are they currently adapting? What is the role of humans within cyber security nowadays? All of these questions stem from the fact that despite our technological advances our systems still appear to be just as vulnerable as ever. Real time visibility in global cyber-attacks is provided by multiple organizations. Norse, [12] FireEye, [13] SUCURI, [14] Wordfence, [15] Kaspersky, [16] Check Point, [17] Trendmicro, [18] and Akamai [19] are some of the fine examples out there, keeping track of different attack origins, types, and targets, for example worldwide DDoS attacks, industries under attack, brute force attacks, attacks blocked by installed anti-virus, botnet activity, and much more. Broadly glancing at the Norse and Kaspersky maps quickly reveal an average of 3 attacks per second occur globally. And that is only what those two organizations measure. In reality, the attack rate might be actually higher. To compliment this, an ongoing list by the Centre for Strategic & International Studies keeps track of all significant cyber incidents since 2006, which reveals lots of pages of mostly cyber incidents regarding global governments and affiliated. Similarly,informationisbeautiful.net [20] draws information from DataBreaches.net and presents an ongoing graph from 2004 onward about the world biggest data breaches with losses greater than 30.000 records, revealing a nearly exponential grow in data breaches and affected persons per year. The amount of people affected by these breaches is astonishing, with the biggest breaches involving tens and hundreds of millions [21] up to a one-time 3 billion involved. [22]

1.5 The blurring lines between inside jobs and external hacks

Closer inspection upon the world's biggest data breaches informs us that the ways in which data is leaked differ greatly. Separation is maintained by Databreaches.net and IdTheftCentre between 'accidentally publishing', 'hacks', 'inside jobs', 'lost or stolen device or media', and 'poor security'. [23] Distinction is apparent here between what appears, on the one hand, as

[12] http://map.norsecorp.com/#/
[13] https://www.fireeye.com/cyber-map/threat-map.html
[14] https://sucuri.net/security-reports/brute-force/?clickid=Vl-x9vx3XX6ZUlIw7M1E0zU3Ukj28VQyly8C3E0
[15] https://www.wordfence.com/
[16] https://cybermap.kaspersky.com/
[17] https://threatmap.checkpoint.com/ThreatPortal/livemap.html
[18] https://www.trendmicro.com/en_us/security-intelligence/breaking-news.html
[19] https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp
[20] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
[21] https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
[22] https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1
[23] https://docs.google.com/spreadsheets/d/1Je-YUdnhjQJO_13r8iTeRxpU2pBKuV6RVRHoYCgiMfg/edit#gid=1

traditional hacking and, on the other hand, forms of human clumsiness and intentional inside leaking.

1.5.1 Accidental human error

This distinction is still pretty vague however. Let us see for example what happened during a 'traditional hack': the Target hack of 2013. This hack resulted in the compromise of 70.000.000 customers' information with 40.000.000 credit card numbers stolen by a supposed Ukrainian hacker group. [24] It cost the company $162.000.000 total in expenses. [25] The hack was performed by stealing credentials from a trusted third party: Fazio Mechanical Services, whose system had access to Targets network to monitor and maintain their systems from afar. The credentials were stolen by a spear phishing attack, which is a more direct form of phishing where pre gathered information is used to personalize the attack, making it more likely to succeed. [26] In line with the reporter willingly (but unknowingly) giving access to her Russian hacker, it appears that all of the technical aspects - the malware reproducing itself within the code of Targets system, stealing data and redirecting it to compromised servers - was preceded by a human error: clicking an infected link, basically granting the hacker permission inside the system. Knowing this, it could be argued that it 'feels' less of a true hack than for example a brute force attack. These examples showcase that there is another side to hacking, comprised of a more enabling human factor. Above, we have seen how accidental human error and how hackers who understand human's place within an organizations IT system can be a major threat. This will be elaborated upon further in the literature review, but as of now it is important to understand that accidental threats refer to situations in which damage or data loss occurs as a result of an insider who has no malicious intent. [27]

1.5.2 Malicious human error

Next to accidental threats, there are also malicious human threats. Malicious threats refer to deliberate attempts by an insider to access and potentially harm an organization's data, systems or IT infrastructure. [28] As technology advances in being able to protect organizations better as time goes by, other means to ensure malicious access are explored. [29] One of these other means to gain access is through seeking 'help' from the inside or by exploring clever tactics to enable help from the inside. Generally described as 'social engineering': the art of using psychology instead of technology to gain access to systems or data, [30] these 'new' (old tricks applied in a new cyber field) tactics open up a more social means of gaining access through what previously was thought only possible through technology. Through these social and technical methods, a blurring of lines between what truly constitutes as a 'hack' becomes

[24] http://people.carleton.edu/~carrolla/index.html
[25] https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/ ; http://people.carleton.edu/~carrolla/story.html
[26] http://searchsecurity.techtarget.com/definition/spear-phishing
[27] https://searchsecurity.techtarget.com/definition/insider-threat
[28] https://searchsecurity.techtarget.com/definition/insider-threat
[29] https://online.maryville.edu/blog/how-to-keep-up-with-constantly-changing-cybersecurity-threats/
[30] https://computerworld.nl/security/100431-social-engineering-praktijkvoorbeelden-en-tips

apparent, as it is difficult to assess these developments as pure external events. Academic works and definitional debates arise on what constitutes as an internal or external hack, [31] and from a business perspective risk and threat management try to keep up with these events to manage their risks accordingly. [32] It is not solely the external hacker that seeks to manipulate insiders however, that is a threat agent, but also the insider himself, that can have the malicious intention of harming his own organization. Thus, the topic of the insider threat is brought up. Generally, the insider threat can be defined as:

"The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization". – CERT 2017 [33]

This definition is rather broad. For example, it does not encompass issues such as groups of individuals that could pose a threat. It does also not mention the way through which the internal and external could join up one way or the other to cause harm as discussed above on accidental and malicious human error. Knowing that the human aspect is of vital importance for cyber security however is something that should be taken from this chapter. In the literature review we will discuss the ramifications of the insider threat more in depth.

1.6 The research question

With both the human and technical side often intertwined, and like in the examples above certainly not mutually exclusive, how can we approach this human factor in cyber security from an analytical point of view? To what extent is the human factor so enabling in the cyber realm and how can we analyse this? What is it exactly that we want to find out when we concern ourselves with the human factor in cyber security? Most of the value that I expect to add towards the current scientific research, and also slightly towards contemporary in the field practices, is insight in how contemporary scientific insights are being applied in the contemporary field. As we will see, we know certain things about the human factor, but are these insights applied in the field? Do we learn from them? And how can we better analyse and understand them? How can we mirror scientific insights and in the field practices in an analytical way? This question seeks to be answered through my research question: through a multi-disciplinary approach comprised of information system security theory and criminology models, to what extent are contemporary scientific insights regarding cyber security with a focus on the insider threat applied in organization's policies?

1.7 Structure of the thesis

In order to approach this problem, at first I will present a literature review in the chapter below, which approaches the problem through established theoretical works about information security and the human factor, as well as new insights with the insider threat remaining as an important aspect. These new insights stem from grounded criminological

[31] I. Loader, S. Percy, *Bringing the 'outside' in and the 'inside' out: crossing the criminology/IR divide,* in Global Crime, 13(4), (2012), 213 – 218
[32] S. L. Moskowitz, *Cybercrime and Business: Strategies for Global Corporate Security* (Cambridge 2017), 191
[33] https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

theoretical works that occupy themselves with information security and human behaviour. The human factor encompasses many things, from victims to perpetrators, this is why the insider threat is so important: it can constitute both and is sometimes in between. These criminological works occupy themselves largely, but not exhaustively, with matters of intention, motivation, opportunity, accidentiality and maliciousness. Combining these with information security grants us a way to approach the human factor and insider threat in a more holistic way and will improve the way to test in what matter these insights are applied in the contemporary field. I will refrain from transitioning too far into the realm of social engineering tactics as this is another subject equally worthy of consideration on its own merit. Though I mentioned technology and human factors are often intertwined in the cyber security field, the focus will remain on the human aspect. This is done to ensure focus. It should not be viewed as a disqualification of technical aspects or not being deemed as equally important, it means that technical aspects will not be the focus of this thesis and therefore sometimes lack the elaborate description they would otherwise deserve, with the simple reason being the focus area of this thesis, as well as the others works used within this thesis that lack a severe technical aspect and use a human factor locus. As we will see in the results of this thesis, the technical aspect of cyber security is very important and equally worthy of attention as it is often lacking in organization's cyber defences, but this area remains open for other work. The framework provided here will thus be created through theory from multiple angles considering the human factor of cyber security, drawing upon conventional and more behavioural theories and ongoing discussions instead of singular ones in order to provide a multi-dimensional base.

Next, I will present my methodology. Here I will explain the choices that I made and thread further into detail about my approach towards answering the research question. I will argue about my use of a qualitative method instead of a more traditional quantitative method and the pros and cons that come with this approach. I will also present the steps I took towards constructing a questionnaire, and discuss the choices I made when considering who to interview for my methods. This will be followed by a page of interview results, which I will then directly mirror against the framework that I constructed in the literature review. Here, I will analyse how academic insights are or are not present in the contemporary cyber security field and what this means and/or implies. Afterwards, the conclusion follows, where I briefly repeat the research question and answer it. This will be followed by a short list of recommendations, providing some insights, and proposing possible research from here onward. The bibliography follows suit.

Chapter 2: Literature review

By examining the research question's components , we can determine a few aspects that are important to elaborate upon before we start off as they did not explicitly appear in the introduction. At first, I would like to further explain the organization component, as well as what exactly is being protected when we talk cyber security and how contemporary problems are a relevant focus area here. After that I will elaborate further on the insider threat, as well as the criminology models, and present a framework of the constructs that I use to reflect on contemporary policies within organizations concerning this insider threat.

2.0.1 Organizations

In the research question I ask if organizations apply academic insights in their cyber security. This has a specific reason. Organizations, or businesses, are not exclusively targeted by cybercrime. However, my goal to target organizations or businesses is tied to the intention of the people that target them. The MICE method explains how the motivation of individuals at the fundament of most spy cases can be tied to the factors of money, ideology, compromise, and ego. [34] It is important to note that if we take for example money as a motivating factor a profit – driven hacker, [35] (s)he will most likely target the most profitable source with businesses being an extremely plausible target. While targeting home users of computers might appear to be a better idea because they are probably more vulnerable than organizations with a cyber defence budget, [36] the most impactful but also lucrative hacks remain to be organizations as the data they are protecting is more valuable and often also tied to personal information of home users that can be exploited to generate revenue, for example credit card information. [37] The hacker's intention is important here. There is no real scientific debate on whether hackers will target something or not. Targeting seems to be directly tied to intention, means and a general consensus arises that potential targets include just about anybody with a connection to the internet or in possession of valuable assets in some digital way. [38]

Next to the attractiveness of businesses for hackers to target, from an academic point of view, businesses, especially with a dedicated cyber department, have access to data indicating how successful and unsuccessful they are in countering cyber threats and have a higher likelihood to be able to provide relevant and more accessible data for research than random home users. Leaving a detailed analysis of hacker motivation behind us, we can see that the reasons for hacking either home users or organizations do not differ or vary that greatly. [39] Their reasons: often financial, nation – state sponsored, (corporate) espionage, hacktivism,

[34] https://www.pri.org/stories/2016-07-13/center-most-spy-scandals-you-can-usually-find-one-these-four-factors

[35] P. T. Leeson, C. J. Coyne, *The Economics of Computer Hacking*, in Journal of Law, Economics & Policy (2005), 511

[36] N. Kumar, K. Mohan, R. Holowczak, *Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls,* in Decision Support Systems 46, (2008), 254

[37] http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

[38] https://cyberpolicy.com/cybersecurity-education/what-type-of-organizations-do-hackers-target-the-most ; https://www.quora.com/Whom-do-hackers-usually-target-and-why ;

[39] https://www.csoonline.com/article/3267988/hacking/what-hackers-do-their-motivations-and-their-malware.html

resource theft, or even intrinsic motivation such as enjoyment, [40] can be divided roughly into general terms such as 'fame', or 'profit'. [41] With reasons, and implicitly also methods such as: social engineering, soft – and – hardware vulnerabilities, browser attacks, password attacks, macro's, DDOS or physical attacks, being somewhat the same, although their scale may vary depending on the target, I deem organisations to be an extremely relevant academic target for answering the question how we can improve cyber security. That being said, there is an incredible amount of study being done about types of hackers and their motivation, [42] which is sadly a scope too big to be incorporated within this thesis. Though I understand the importance hacker motivation and the tools that they use, even going as far today as constructing a personality and trait profile to counter hackers, [43] the scope of this thesis is to compare how academic insights manifest themselves in the cyber security field. As will be explained later, this will encompass a behavioural based approach, combining several different angles and studies done in the ISS field.

2.0.2 Cyber security, what it means, and what it protects

So what exactly encompasses this cyber security field and what exactly needs to be protected? Organizations can possess information in the form of data as an asset. Currently, international competition has made an organization's proprietary information more valuable than ever. [44] Information security management can therefore focus on the protection of information as an asset. [45] Data is not the only valuable sought after by attackers however. Devices purely connected to the internet, even if they are completely devoid of any data are often good targets for hackers due to their connectivity to other devices and services, as well as their deeply interwoven position in our lives and society. [46] These 'Internet of Things', carry a vast threat implication that is not often noticed. [47]. When looking at profit or pride as a motivator, a hacker might feel more accomplished hacking a big organization instead of random nobodies, or it might yield him a better perceived profit. And speaking of profit, pure monetary gains can also be an extreme motivator for any hacker. In combination with social

[40] K. R. Lakhani, R. G. Wolf, *Why Hackers Do What They Do: Understanding Motivation Effort in Free/Open Source Software Projects,* in MIT Sloan School of Management Working Paper 4425-03 (2003), 5, 16 – 18
[41] P. T. Leeson, C. J. Coyne, *The Economics of Computer Hacking,* in Journal of Law, Economics and Policy, 1(2), (2005), 511, 517 – 531
[42] A. T. Norman, *Computer Hacking Beginners Guide: How to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack* (ACM Digital Library 2018) ; G. Thomas, G. Low, O. Burmeister, *"Who Was That Masked Man?": System Penetrations – Friend or Foe?*, in Cyber Weaponry (2018) ; N. L. Beebe, V. S. Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process,* in Communications of the Association for Information Systems, 26(17), (2010)
[43] M. Odemis, C. Yucel, A. Koltuksuz, *Suggesting a Honeypot Design to Capture Hacker Psychology, Personaility and Sophistication,* in ICCWS 2018 13th International Conference on Cyber Warfare and Security (2018)
[44] T. L. Wiant, *Information security policy's impact on reporting security incidents,* in Computers & Security 24, (2005), 449
[45] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security 24, (2005), 473
[46] M. Abomhara, G. Koien, *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,* in Journal of Cyber Security and Mobility, 4(1), (2015), 65
[47] M. J. Covington, R. Carskadden, *Threat implications of the Internet of Things,* IEEE, Cyber Conflict (CyCon), (2013), accessed on http://ieeexplore.ieee.org/abstract/document/6568380/

engineering, elaborate schemes are produced where the sole motivator is profit in monetary form. [48] Reputation is another driver, that might sometimes be overlooked. A business that relies on a good reputation in order to exist or make profit can be ruined after a costly or embarrassing cyber incident scaring off not only existing or potential customers, but also shareholders. [49]

What about the protection of the data itself? Guiding scientific theory is related to ways in which data protection is managed. The first and most obvious link is through information security theory. Not as much so defined as one theory, but rather a method featuring a multitude of theories, models and frameworks through which solutions and guidelines are suggested to fill information security research through human and technical issues. Thus they feature effective principles and guidelines for what are conceived as the best practices in information security and information security management, all to develop solutions for the related problems. [50] Therefore we are looking for solutions to in-the-field problems instead of actively engaging in epistemological scientific debate. This does not mean there is no relevant scientific debate present however. Propositions are already being made to redefine information security to divide 'soft issues' such as human, organizational, culture, ethics, policies, law, and more technical issues due to the problems the standardized 'CIA' (Confidentiality, Integrity, and Availability)[51] definition brings. [52] Topics such as Information Security Awareness (ISA) and Information Security Policy (ISP) offer multiple scientific angles towards working with any type of Information System and the many ways of protecting that data. [53] Decision making and risk assessment models feature a way of coping with modern day problems regarding IS security. [54]

In order to not get confused in all of this, it is important to bring up some definitional work. Cyber security is often referred to "the protection of internet-connected systems, including hardware, software and data, from cyber-attacks", [55] or more elaborately along the lines of: " The body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access". [56] As such, it encompasses multiple facets such as application security, information security, network security, recovery, continuity, operational security, and end-user education. Whether the data is sensitive information, intellectual property, financial data, personal information, there is a

[48] https://www.cio.com/article/3136159/security/how-to-prevent-ceo-fraud.html
[49] https://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html
[50] S. Ada, *Theories Used in Information Security Research: Survey and Agenda,* in Handbook of Research on Social and Organizational Liabilities in Information Security (New York 2009), 1 – 14
[51] S. H. von Solm, *Information Security Governance – Compliance management vs operational management,* in Computers & Security 24, (2005), 444
[52] B. Lundgren, N. Möller, *Defining Information Security,* in Science and Engineering Ethics (2017),
[53] A. Tsohou, S. Kokolakis, M. Karyda, E. Kiountouzis, *Investigating Information Security Awareness: Research and Practice Gaps,* in Information Security Journal: A global Perspective, 17 (2008), 207 – 210 ; A. W. Kadam, *Information Security Policy Development and Implementation*, in Information System Security, 16(5), 2007, 246
[54] D. W. Straub, R. J. Welke, *Coping with Systems Risk: security planning models for management decision making,* in MIS Quarterly, 22(4), (1998), 441 – 469
[55] https://searchsecurity.techtarget.com/definition/cybersecurity
[56] https://digitalguardian.com/blog/what-cyber-security

way to secure it and cyber security deals with this aspect. IS (Information Security or infosec) or ISS (Information System Security) are thus part of cyber security. IS is defined as "a set of strategies for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and non-digital information". [57] It is designed to "protect the confidentiality, integrity, and availability of computer system data from those with malicious intentions". [58] This triad is known as the 'CIA' method, where confidentiality stands for rules that limit access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is the guarantee of reliable access to the information by authorized people. [59] This triad is often cited as the reason or definition for information security, and is referred toward itself and its elements (hardware, software, information, people, and processes) as part of IS security. [60] Therefore, when we talk about cyber security of an organization, or its information security, both are often used in conjunction, even in the professional field. Both apply towards strategies, processes, tools and policies.

2.0.3 Contemporary problems and hacker adaption to counter measures

Knowing now that the motivation of hackers can vary, as well as what they seek can vary, and therefore what organizations want to protect can vary, we can also understand that the methods that hackers will use can vary. Generally, it is known that criminals evade detection by modifying known attacks. [61] This modification can also imply working around traditional known counter measures that protectors design. [62] Despite recurrent successes of 'old hacking tactics', such as for example ransomware or Trojan horses, the individual variants are often quickly taken care off and will not result in much success after cyber defence has caught up with them. [63] Realising that old vulnerabilities will probably be patched and no longer possess any danger, with exceptions here and there, the focus on recurrent vulnerabilities and also future implications toward those vulnerabilities is a must. By looking at modern, sometimes current year, contributions in academic works but also in the field information I strive to produce a relevant framework of analysis comprised of constructs that are to be empirically measured. The overarching theme of the threats will come from insider threat and human

[57] https://searchsecurity.techtarget.com/definition/information-security-infosec
[58] https://www.techopedia.com/definition/10282/information-security-is
[59] https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA ; J. M. Anderson, *Why we need a new definition of information security,* in Computers & Security, 22(4), (2003), 308 ; R. von Solms, J. van Niekerk, *From information security to cyber security,* in Computers & Security, 38, (2013), 98
[60] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 473
[61] T. H. Ptacek, T. N. Newsham, *Insertion, Evasion and Denial of Service Eluding Network Intrustion Detection*, in Technical Report Secure Networks Inc., 1998) ; P. Szor, *The Art of Computer Virus Research and Defense,* in Addison – Wesley Professional (2005) ; K. Julish, *Understanding and overcoming cyber security anti-patterns,* in Computer Networks 57 (2013), 2208
[62] A. Appari, M. E. Johnson, *Information security and privacy in healthcare: current state of research,* in International Journal of Internet and Enterprise Management, 6(4), (2010),
[63] R. Richardson, M. North, *Ransomware: Evolution, Mitigation and Prevention,* in International Management Review, 13(1), (2017), 11 – 13, 17

factor perspective, rather than a focus on external hacker tactics, while duly noting that these themes might often cross in the field. [64]

The cyber related threats with the focus on the human factor are the major determinant factor in this thesis. I will now shortly explain why this focus is deemed so important and is of utmost relevance for businesses and organisations seeking protection in their computer and information security (CIS). In essence, a long running 'debate' within CIS exists about information security being a people problem, rather than a technical one. [65] Debate is put in parentheses here, because it seems to be not much of a debate as it is for a continuous calling of attention over the years to respond to an insufficient number of experts in dealing with the human factor in information security. Basically, it is argued that cyber security becomes an inter-disciplinary field where success depends on factors such as technology, but also beyond it, such as economics, usability, and psychology. [66] This appears at first sight to heavily conflict a traditional view that information security should only include technical aspects. [67] However, the academic world seems to be relatively well up to date considering the multi-dimensional approach towards the protection if information systems. Why, then, despite this surge of knowledge and the combined investments done through technical measures are there still major security weaknesses in today's information systems? [68]

2.1.0 The insider threat

To answer the above question is to approach the main research question. In order to provide a solid analytical framework, I will be using various already well established theories within the IS and CIS field to provide a multi–dimensional, or holistic, approach. Information systems in an organizational context are best expressed as a combination of technology, people, and management. [69] Amongst these three factors, people play a key role in the process of IS security and can be the weakest link at the same time. [70] In a more general sense, it can be argued that security in itself is a people problem, which means in the case of cyber security: leaving people in control of technology, not vice versa. [71] At first, let us begin by looking at one of the most important bodies of knowledge currently within the IS and CIS field: the insider threat.

2.1.1 How the largest threat comes to be

[64] https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack ; https://www.ipexpoeurope.com/2018-Seminars/Cyber-Security-Keynote/Thursday-04-October-2018/Real-cases-of-social-engineering-hackers-competitors-and-insiders
[65] E. Schultz, *The human factor in security,* in Computers & Security 24 (2005), 425
[66] K. Julisch, *Understanding and overcoming cyber security anti-patterns,* in Computer Networks 57, (2013), 2211
[67] W. Pieters, *The (Social) Construction of Information Security* in The Information Society, 27 (2001), 326
[68] K. Julisch, *Understanding and overcoming cyber security anti-patterns,* in Computer Networks, 57(10), (2013), 2206
[69] L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013), 447
[70] J. J. Gonzalez, A .A. Sawicka, *framework for human factors in information security,* in Paper presented at the World Scientific and Engineering Academy and Society (WSEAS), Rio de Janeiro, (2002)
[71] E. Schultz, *The human factor in security,* in Computers & Security, 24, (2005), 426

The theory of the malicious insider holds that within organizations, the insider has the potential to cause more damage than an outside attacker. [72] As we have seen, despite rising costs the security of organizations continue to show ineffective or counterproductive patterns of security. [73] These security failures can have a psychological, technical, and organizational aspect,[74] and can be summarized as follows: [75] (1) an overreliance on intuition to make security decisions, (2) weak security governance, (3) leaving cracks in the security foundation, (4) overreliance on knowledge versus intelligence. Overreliance on intuition for making security decisions refers to the variables decision makers have to take into consideration when prioritizing security investments. For instance, the probability of a cyber-attack, the effectiveness of existing countermeasures and the impact or costs of the attacks should be taken into consideration. This decision making process is filled with bias, which might lead to suboptimal decisions with confirmation bias (ignoring evidence that contradicts a preconceived belief) being a major aspect. Weak security governance refer to who determines desirable behaviour in using the organization's IT, who has decision rights and who has accountability. Not having clear defined roles, responsibilities, priorities and processes is hurtful for the ability to withstand cyber-attacks. Leaving cracks in the security foundations refers to the struggle an organization can have to implement a consistent baseline level of security, which includes foundational security controls. Overreliance on knowledge versus intelligence refers to both the pre-emptive and reactive nature of security. Knowledge of specific attacks fuel security, but only responding to known attacks keeps an organization vulnerable and makes a knowledge based approach too static. These patterns give a slight hint towards why modern day cyber security efforts are stagnating, [76] but do not offer a sufficient explanation alone.

2.1.2 Technology, organization, and psychology

We have so far seen how generally speaking technology, organization, and psychology can play a role. Technology based solutions are interesting on their own, both in a pre-emptive and reactive way. They focus heavily on software and hardware solutions, such as auditing, layered access systems, access control, databases, servers, network security reviews, firewalls, malware detection, [77] two factor authentication, biometric solutions, machine learning

[72] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 187

[73] K. Julisch, *Understanding and overcoming cyber security anti-patterns*, in Computer Networks, 57, (2013), 2206

[74] K. Julisch, *Understanding and overcoming cyber security anti-patterns*, in Computer Networks 57 (2013), 2207

[75] K. Julisch, *Understanding and overcoming cyber security anti-patterns*, in Computer Networks 57 (2013), 2206 – 2211

[76] K. Julisch, *Understanding and overcoming cyber security anti-patterns*, in Computer Networks 57 (2013), 2211

[77] http://www.sng.za.com/advisory/integrated-technology-and-governance-solutions/information-communication-and-technology-advisory/information-technology-security-solutions ; Z. Rezaee, A. Sharbatoghlie, R. Elam, P. L. McMickle, *Continuous Auditing: Building Automated Auditing Capability,* in D. Y. Chan, V. Chiu, M. A. Vasarhely, (eds.), *Continuous Auditing theory and application* (2018), 169 – 190

solutions, the possibilities are endless and ever increasing. [78] Recognizing the importance of technical solutions, this thesis will not focus on technical solutions to the cyber issues addressed, but instead divert its attention towards the organizational and psychological aspects. As we will see, general deterrent factors will include some technical solutions, but they serve the purpose of contributing towards organizational or psychological counters instead of being investigated as a means on their own. It is important to understand that security and control are there to ensure that organisational systems retain their integrity, confidentiality, and availability. [79] In the end, despite having an abundance of useful technological means to ensure information security, human error in any form still leaves opportunity to bypass or defeat these counter measures. [80]

2.1.3 Types of insiders and the impact of technical, business, social and cultural factors

Returning to the insider threat, we see that it refers to threats originating from people who have been given access rights to an information system and misuse their privileges, violating the IS security policy of the organization. [81] They can for example be classified in groups of pure insider, insider associate, insider affiliate, and outside affiliate (not an insider). [82] The categorizations are important in their own respective field, but of not too great importance within this thesis, as it constitutes another body of literature. It is important however, to understand that each category comes with different privileges and different positions within organizations. The pure insider often has the highest level of access and consists of 'pure' employees, in the sense that they are directly tied to the company. Insider associates are often contractors and/ or third party personnel, while inside affiliates are often not directly tied towards the company, but affiliated with those who are.

Knowing that there are different categorizations of insiders is important considering how insider risk can be examined in the context of changing technical, social, business, and cultural factors. [83] These factors carry with them certain implications on the insider threat, and differ per categorization. The social and technology factor that is affecting insider threat can be seen as the ever developing and ever increasing usage of technology, which makes its way

[78] E. Toch, C. Bettini, E. Shmueli, L. Radaelli, A. Lanzi, D. Riboni, B. Lepri, *The Privacy Implications of Cyber Security Systems: A Technological Survey,* in ACM Computing Surveys, 51(2), (2018), 7, 9, 15 – 17 ; W. B. Glisson, K. K. R. Choo, *Introduction to the Minitrack on Cyber – of – Things: Cyber Crimes, Cyber Security and Cyber Forensics,* in Proceedings of the 561st Hawaii International Conference on System Sciences (2018), 5574 – 5575 ; K. Nakao, *Proactive cyber security response by utilizing passive monitoring technologies,* in IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, (2018) ; K .K. R. Choo, M. Bishop, W. Glisson, K. Nance, *Internet – and cloud – of – things cybersecurity research challenges and advances,* in Computers & Security, 74, (2018), 275 – 276 ; G. B. Magklaras, S. M. Furnell, *Insider Threat Prediction Tool: Evaluating the probability of IT misuse,* in Computers & Security, 21(1), (2001), 62 – 73

[79] G. Dhillon, J. Backhouse, *Current directions in IS security research: towards socio-organisational perspectives,* in Information Systems Journal, 11, (2001), 135, 147

[80] E. Schultz, *The human factor in security,* in Computers & Security, 24, (2005), 425

[81] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 473

[82] K. R. Sarkar, *Assessing insider threats to information security using technical, behavioural and organisational measures,* in Information Security Technical Report, 15, (2010), 115

[83] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 186, 189 - 191

towards the work floor. With increased usage however, comes increased risk. An example could be personal use of workplace technology, resulting in increased risk by visiting unsafe sites. Over the years ,more and more technological devices that merge home and work lives appear and are used on office grounds. [84] Security policy, controls, guidelines and training can often not keep up with these changes. [85]

Business and economic factors affecting the insider threat are also tied with a changing business world. One of the most notorious changes in the business world is the process of outsourcing. The involvement of a third party given access to systems and information brings a new kind of insider risk with it. [86] Research also shows that the recent global economic recession can affect certain malicious behaviour and has direct implications for an increase on insider attacks and insider threat at various levels of organizations. [87] At processes where trust and loyalty are expected, or even necessary, budget cuts and pay freezes might impact employees in the long run, leaving the recession and its consequences to change behaviour and have direct implications for insider attacks. [88]

Cultural factors affecting the insider threat regard certain aspects of organisational, but also national and/or regional culture. What this means, is that organisational, national, or regional culture can include and affect perceptions and behaviour towards crime and security. [89] Culture can cause fear uncertainty and doubt in the wrong situations. An example could be if an organization or company does not allow you to speak up against your superiors, if said superior is wrong in his risk assessment, serious threat can emerge if nothing is corrected or able to be rectified. Regional and national attitude towards crime and the means of protection against it can exert serious pressure at the work floor. Acceptable norms for doing business can differ from region to region and country to country. Practices that are considered immoral or downright illegal, for example bribes, can be common and/or accepted in other parts of the world. [90] Considering all these factors, we can see a pattern where the social environment is of direct influence toward potential insider incidents. It appears that organisations struggle with employees (and/or staff for that matter), who attempt to improve their own financial position or career path, resulting in less affinity, a lose loyalty, and a difficulty adhering to organisational policy and guidelines. Changes to the nature of doing

[84] J. Kavanagh, *Security special report: the internal threat,* in Computer Weekly (2006)
[85] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 189 ; A. Mohamed, *CW security trends for 2009,* in Computer Weekly (2009) ; J. Kavanagh, *Security special report: the internal threat,* in Computer Weekly (2006)
[86] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 190
[87] McAfee, *Virtual Criminology report* (2008) accessed on https://resources2.secureforms.mcafee.com/LP=2980 ; A. Mohamed, *CW security trends for 2009,* in Computer Weekly (2009) ; P. Guerra, *How Economics and Information Security Affects Cyber Crime and What It Means in the Context of a Global Recession,* in BlackHat 2009 Turbo Talk Whitepaper (2009), 1 – 6 ; A. Savvas, *Big increase in cybercrime, and recession will make it worse,* in Computer Weekly (2008)
[88] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 190
[89] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 190 – 191
[90] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 191

business has affected the direct control that organisations have on their own structure and culture, and the various levels of trust and relationships that can be developed. [91]

2.1.4 The disgruntled employee

Thus we can see that in these changing aspects, different categories of insiders can have different ramifications and implications upon their own threat and risk. An insider that is not 'pure' and underpaid might for example not be as dangerous as a pure insider that is underpaid. But there could always be exceptions, differing from person to person: it is difficult to find a common profile. [92].

As the above information suggests, the 'disgruntled employee' seems at first sight like a prime focus area to gain traction on reducing the insider threat. It would appear however, that research shows this could be a stereotype and that there is no correlation between disgruntled workers and insider threats. [93] It should be noted however that the NIAC (National Infrastructure Advisory Council) investigated critical infrastructures as opposed to for example businesses. This has implications for the reasons an employee might 'betray' their employer, when looking at factors such as career path and monetary gain or for example any worthwhile information to steal and redistribute. There is also no mention in the report considering cases of revenge, which seem to be a top intended effect of the potential malicious insider, as we have seen before together with power, control, and financial gain, in other research. [94] Therefore, looking at the disgruntled employee might prove to be very worthwhile. It is in fact a realistic problem within the cyber security business and should definitely be considered in threat assessments. [95]

2.1.5 From detecting actual threats to pre-emptive identification

Disgruntled employees are not the sole focal point of the insider threat however. As mentioned earlier, any type of human error can result in bypassing security measures. The insider comes in many forms and thus represents a broad spectrum of potential threats. It can therefore be rewarding to explore the link between potential and actual threat, as well as between threat and malicious action. Attempting to detect shifts towards malicious action can be done by identifying the warning signs for insider behaviour, as well as taking appropriate action to resolve problems. Both of these require time, effort, investment, and commitment. [96] These can be balanced out by exploring a holistic approach or perspective. By embracing this perspective, minimal technical controls such as encryption, access control, privilege,

---

[91] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 191

[92] M. R. Randazzo, M. Keeney, E. Kowalski, *Insider Thread Study: Illicit Cyber Activity in the Banking and Finance Sector,* in NTACUSSS, *Networked Systems Survivability* (Carnegie Mellon 2005), 15

[93] NIAC, *HMG IA standard No. 1, technical risk assessment part 1,* Issue 3.2 (October 2008)

[94] https://www.helpnetsecurity.com/2018/05/15/insider-threat-blind-spot/ ; https://threatconnect.com/blog/how-to-explain-what-is-a-cyber-threat/ ; https://scramsoft.com/revenge-hacking-is-the-new-black-in-the-cybercrime-underworld/

[95] https://insights.sei.cmu.edu/insider-threat/2015/07/handling-threats-from-disgruntled-employees.html

[96] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 191

monitoring, auditing, reporting, and many more, can be balanced out against non-technical factors, usually involving perceptions, expectations and implementation, and enforcement of security policy, as well as behavioural and organizational techniques. [97]

This holistic approach, despite being very broad, does help in addressing certain grey areas and establishing accountability for actions and setting expectations and boundaries for employees through guidelines and a formal policy. Threading further into detail is often done by risk assessment and/or risk modelling of some kind. [98] Within these models, the human threat is often decomposed in factors that can be included in an insider threat assessment, and will help to identify mitigation controls that can assume either technical or procedural measures, or a combination of both. [99] Traditionally, automated detection of high risk behaviour are a preferred method used in these holistic approaches. [100] This does not mean that there is no room for human factors within the automatic responses, it does mean that technical measures are a preferred method of enabling automated response. From an academic perspective, there is a substantial amount of calls towards improving security through the human factor, however [101] introducing methods that feature technical, behavioural, organizational, or a combination of these three. [102] Behavioural assessment can be done for example by constructing a psychological profile of the employees, or by actively tracking some form of norm for a company culture. Technical assessments often involve a technical

[97] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 193 ; K. R. Sarkar, *Assessing insider threats to information security using technical, behavioural, and organisational measures,* in Information Security Technical Report, 15(3), (2010), 112

[98] N. Baracaldo, J. Joshi, *An adaptive risk management and access control framework to mitigate insider threats,* in Computers & Security, 39, (2013), 238

[99] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 193

[100] F .L. Greitzer, R. E. Hohimer, *Modeling Human Behavior to Anticipate Insider Attacks,* in Journal of Strategic Security, 4(2), (2011), 25, 42 – 43

[101] E. E. Schultz, *A framework for understanding and predicting insider attacks,* in Paper to be presented at Compsec 2002, London 30 October (2002), 531 ; A. D. Veiga, J. H. P. Eloff, *A framework and assessment instrument for information culture,* in Computers & Security, 29(2), (2010) ; A. Alhogail, *Design and validation of information security culture framework,* in Computers in Human Behavior, 49, (2015) ; https://patents.google.com/patent/US9930062B1/en ; M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, D. Gritzalis, *An Insider Threat Prediction Model,* in S. Katsikas, J. Lopez, M. Soriano, (eds.), Trust, Privacy and Security in Digital Business (Berlin 2010), 26 – 37 ; F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, R. E. Hohimer, *Identifying at-risk employees: modelling psychological precursors of potential insider threats,* in proceedings of 45th Hawaii International Conference on System Sciences (Maui 2012), 2392 – 2401 ; V. Stavrou, M. Kandias, G. Karoulas, D. Gritzalis, *Business Process Modeling for Insider Threat Monitoring and Handling,* in C. Eckert, S. K. Katsikas, G. Pernul, (eds.), Trust, Privacy, and Security in Digital Business (Cham 2014) ; D. Liu, X. F. Wang, J. Camp, *Game-theoretic modelling and analysis of insider threats,* in International Journal of Critical Infrastructure Protection, 1, (2008), 75 – 80 ; P. Legg, N. Moffat, J. R. C. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith, S. Creese, *Towards a conceptual model and reasoning structure for insider threat detection,* in Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(4), (2013) ; N. Baracaldo, J. Joshi, *A trust-and-risk aware RBAC framework: tackling insider threat,* in SACMAT'12 Proceedings of the 17th ACM symposium on Access Control Models and Technologies (Newark 2012), 167 – 176

[102] K. R. Sarkar, *Assessing insider threats to information security using technical, behavioural, and organisational measures,* in Information Security Technical Report, 15(3), (2010), 130 – 131 ; C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 193

solution, such as tracking, logging, authentication, an intrusion detection system, honeypots (divertive servers that attract malicious behaviour but to not contain anything of value), automated action cycles, and many more. Organizational assessments can include for example an unintended behaviour report system, weekly security audits, or endorsing a certain wanted office culture. Organizations thus are currently dealing with modelling of human behaviour within the information security business. Attempting to explain the link between a potential threat and actual malicious action happens trough a holistic encompassing approach that attempts to model the insider threat though psychological or motivational factors that underlie certain behaviour, deconstructing the threat into matters of motivation, opportunity, and capabilities.

2.1.6 The accidental insider versus the malicious insider.

We have seen so far how the insider threat is a relevant and big threat, but what about the nature or intent of their threat? So far, it would appear through my description of the insider threat, that the insider lurks maliciously in the background, waiting to strike at an unsuspecting employer. A more nuanced vision is appropriate however. It would appear that it is not the malicious, but the either careless, uninformed or negligent employee that stands more than half of the times as the root cause of incidents. [103] Insider threat can be categorized into malicious: intentional and adversarial in nature, and non – malicious: accidental, non – adversarial. [104]

To mitigate this human weakness that leads to unintentional harm to the organization, we at first have to return to the notion that technology is often falsely perceived as the immediate answer to IS problems. [105] Information Security can, in some way, be seen as primarily a human factor problem: if a user has poor training, execution, or features other errors, even an ideal software or hardware solution will not be of any use. [106] This argument boils down to an approach where poor usability can severely impact the security of a system. [107] This danger of

[103] https://www.ponemon.org/blog/tag/cost%20of%20insider%20threats ; https://www.observeit.com/blog/new-ponemon-institute-study-insider-threats-lead-to-big-losses-and-significant-costs/ ; https://www.infosecurity-magazine.com/opinions/accidental-insiders-serious-threat/ ; https://newsroom.accenture.com/news/new-report-finds-insider-corporate-data-theft-and-malware-infections-among-biggest-threat-to-digital-business-in-2016.htm ; https://intelligentid.com/75-insider-threats-accidental/ ; https://www.iasplus.com/en/binary/dttpubs/2009securitysurvey.pdf

[104] T. Walker, *Practical management of malicious insider threat – an enterprise CSIRT perspective,* in Information Security Technical Report, 13, (2008), 227

[105] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, G. Giannakopoulos, *The Human Factor of Information Security: Unintentional Damage Perspective,* in Procedia - Social and Behavioural Sciences, 147, (2014), 425

[106] http://trainingtoday.blr.com/article/most-effective-training-techniques/ ; http://blogs.worldbank.org/edutech/worst-practice ; https://www.forbes.com/sites/danwoods/2013/03/11/why-security-without-usability-leads-to-failure/#1c32b7244533

[107] L. M. Mayron, Y. Hausawi, G. S. Bahr, *Secure, Usable Biometric Authentication Systems,* in C. Stephanidis, M. Antona, (eds.), Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for Inclusion. UAHCI 2013. Lecture Notes in Computer Science, 8009, (Berlin 2013), 195 ; S. Hinde, *The law, cybercrime, risk assessment and cyber protection,* in Computers & Security (2003), 93 ; D. D. Caputo, S. L. Pfleeger, M. A. Sasse, P. Ammann, J. Offutt, L. Deng, *Barriers to Usable Security? Three Organizational Case Studies,* in IEEE Security & Privacy, 14(5), (2016)

poor usability can be seen in conjunction with two other aspects: organizational factors, and technological factors. Organizational factors include for example communication, security culture, and policy. [108] Technological factors concern the interplay that they have with the human and organizational factors, instead of pure technological approaches to CIS systems. [109]

In order to limit vulnerable acting of the human factor, the causal history that extends through the many levels of the organization and system must be explored, where conditions arise from decisions made by not only end users, but also management, designers, policy writers and network administrators. [110] It would appear then, that human and organizational factors are indeed related to technical computer and information security vulnerabilities. [111] Simply put, end user failure in correctly operating technology can be seen in a broad perspective that pierces through the organization itself, rather than being seen as intentionally wrong in a vacuum. Therefore, if the usability of a system is bad, or its end users cannot understand and/or operate it, this could indicate a problem exists within the different layers of the organization. What this does not take away, is the potential threat that exists within users themselves, but it can offer a perspective that can be used to approach the problem and make improvements. One study hypothesizes for example that increased difficulty of choices leads to a match of challenges and hacker skills. Action freely follows the previous action here, and the process is in a way unconscious, accompanied by emotions and is self-rewarding. [112] Within the context of the accidental insider, this means an end user could enhance or follow through on unsafe behaviour when he is challenged by difficult choices if said behaviour enables him to do his job. The intention might not be malicious, but the actions are harmful, and thus the accidental insider threat is formed. It is interesting to ponder upon the ramifications of this, such as for example ways to facilitate an uninformed or ignorant attitude of users to be considered as intentional, making wilful ignorance punishable through policy, [113] or by even by law. [114] This remains an organizational aspect however, as it is a legitimate question who bares the responsibility for educating the employees, or perhaps even the employer himself.

2.1.7 Education, security training, and awareness

This brings us to the next aspect, which is the importance of education, security training, and awareness. These are considered to be some of the greatest non – technical measures

[108] S. Kraemer, P. Carayon, *Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists,* in Applied Ergonomics, 38(2), (2007), 143 – 154
[109] R. Werlinger, K. Hawkey, K. Beznosov, *An integrated view of human, organizational, and technological challenges of IT security management,* in Information Management & Computer Security, 17(1), (2009), 4 – 49
[110] S. Kraemer, P. Carayon, J. Clem, *Human and organizational factors in computer and information security: Pathways to vulnerabilities,* in Computers & Security (2009), 517
[111] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, G. Giannakopoulos, *The Human Factor of Information Security: Unintentional Damage Perspective,* in Procedia - Social and Behavioural Sciences, 147, (2014), 425
[112] A. E. Voiskounsky, O. V. Smyslova, *Flow-Based Model of Computer Hackers'Motivation*, in CyberPsychology & Behaviour, 6(2), 2003, 171
[113] https://securityintelligence.com/ignorance-is-no-excuse-but-it-is-reality/
[114] A. Sarch, *Wilful ignorance in law and morality,* in Philosophy Compass, 13, (2018), 1 – 11

available considering human factors and security. [115] User awareness is seen as an essential good practice in business and it can benefit the organization on multiple areas. [116] Users become aware of risks related to the organization's IS and IT departments, as well as becoming familiar with security policies and procedures. Education and awareness can aim to increase the trust by developing an understanding of the reasons for the security policies and controls, which is in everybody's long term interest. [117] Awareness and education can prepare an organization and its employees, but changing behaviour involves breaking habits and establishing new ones through targeted training. [118] Though results may inherently vary considering the true effectiveness of security awareness programs and training, [119] it is undeniable that these programs help in fostering a security culture within organizations. [120] Overall, a general scientific conclusion seems to be, despite the knowledge that security incidents still happen, that education, awareness, and security training yield a positive, security reinforcing effect. [121] It appears that the effectiveness to self-efficacy (belief in a person's innate ability to perform a certain action) and security compliance intention are greatly improved through the influence of security education and training. [122] Effective compliance of security policies, as well as proper integration of "people", "process", and "technology", are often seen as key factors in information security management, and this aspect of education, security training, and awareness is thus generally seen as a positive contributor towards that cause. [123]

2.1.8 The shared burden of responsibility

[115] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 193 – 194

[116] E. Humphreys, *Information security management standards: Compliance, governance and risk management,* in Information Security Technical Report, 13, (2008), 251

[117] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 194

[118] M. A. Sasse, D. Lawrence, L. C. Kemp, D. Ashdenden, I. Fléchais, P. Kearney, *Human vulnerabilities in security systems,* in human factors working group white paper KTN, 7 – 10 accessed on: https://pdfs.semanticscholar.org/38b4/36a07f78056a82df1e9228b87ca145f09f9c.pdf

[119] https://securityintelligence.com/how-effective-is-security-awareness-training-for-threat-prevention/ ; S. K. Katsikas, *Health care management and information systems security: awareness, training or education?* In International Journal of Medical Informatics, 60, (2000), 135 ; B. D. Cone, C. E. Irvine, M. F. Thompson, T. D. Nguyen, *A video game for cyber security training and awareness,* in Computers & Security, 26(1), (2007), 63

[120] https://www.enterprise-cio.com/news/2016/jan/22/importance-security-awareness-training-enterprise-it-governance/

[121] R. S. Shaw, C. C. Chen, A. L. Harris, H. J. Huang, *the impact of information richness on information security awareness training effectiveness,* in Computers & Education, 52, (2009), 99 ; Y. Rezgui, A. Marks, *Information security awareness in higher education: An exploratory study,* in Computers & Security, 27, (2008), 250 – 251 ; A. Pattabiraman, S. Srinivasan, K. Swaminathan, M. Gupta, *Fortifying Corporate Human Wall: A Literature Review of Security Awareness and Training,* in M. Gupta, R. Sharman, J. Walp, P. Mulgund, (eds.), *Information Technology Risk Management and Compliance in Modern Organizations* (2017) , 142 – 175

[122] C. W. Yoo, G. L. Sanders, R. P. Cerveny, *Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance,* in Decision Support Systems, 108, (2018), 113

[123] M. Eminagaoglu, E. Uçar, S. Eren, *The positive outcomes of information security awareness training in companies,* in Information Security Technical Report, 14, (2009), 223, 228 – 229 ; E. Albrechtsen, J. Hovden, *Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study,* in Computers & Security, 29, (2010), 435 – 437

We have now explored the human factor in regards to the perspective of the insider employee. There is a bigger perspective however. The human factor encompasses more than just end user insider threat. Management, and other layers of the organization can also contribute towards the risk. Management can for example provide a too large work load which results in faulty behaviour, or provide inadequate staffing. External influences, faulty management, poor performance, improper resource management, policy issues, lack of training, not rewarding talent, refusing proper security education or training, all can contribute towards increasing the threat an organization faces. Failure of management to adhere to their own responsibilities in cyber security is a serious problem. [124] Throughout the organization, people might lack awareness, belief, engage in faulty behaviour, make inadequate use of technology, or simply lack motivation. In the end, security is everyone's responsibility. [125] It is important that people are aware of the dangers, and understand that they themselves are part of the danger.

2.1.9 Policies

We have seen how the cure to these factors can partially be found in security training and awareness. [126] There is another important key aspect towards handling these problems however. An understandable, well implemented policy is one of the key solutions of countering both accidental and malicious security incidents. [127] A policy that accounts for the objectives of the business and recognizing the business mission is a must, but is often overlooked if it interferes with productivity or generating revenue. [128] The goal is to influence behaviour that is consciously accepted by the employees, in order to secure commitment, [129] but does not stray too far from the business goal and the means to obtain it.

It is important then, that these policies account for accidental behaviour as well. But how can they do this? We can see how policy could adapt for malicious insiders, for example by tracking unauthorized access, destruction of information or assets, theft of information, or sabotage. [130] Malicious insiders can be more knowledgeable than an external attacker and are

[124] J. Morgan, *Board and management responsibilities for information security,* in CIO Information Technology Governance, February 9, (2018) ; https://www.sagedatasecurity.com/blog/cybersecurity-roles-and-responsibilities-for-the-board-of-directors

[125] http://www.cybersecurity.my/data/content_files/11/51.pdf

[126] K. Thompson, J. van Niekerk, *Combating information security apathy by encouraging prosocial organisational behaviour,* in Information Management & Computer Security, 20(1), (2012), 39 – 46 E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, G. Giannakopoulos, *The Human Factor of Information Security: Unintentional Damage Perspective,* in Procedia - Social and Behavioural Sciences, 147, (2014), 427

[127] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, G. Giannakopoulos, *The Human Factor of Information Security: Unintentional Damage Perspective,* in Procedia - Social and Behavioural Sciences, 147, (2014), 426

[128] C. Orshesky, *Beyond technology – The human factor in business systems,* in Journal of Business Strategy, 24(4), (2003), 43 – 47

[129] T. P. Layton, *Analysis of ISO/IEC 17799:2005 (27002) Controls,* in T. P. Layton, *Information Security Design, Implementation, Measurement, and Compliance* (2007), 117 – 123

[130] T. L. Wiant, *Information security policy's impact on reporting security incidents,* in Computers & Security, 24, (2005), 449 - 451

known for being more effective at defeating security controls. [131] So how do we deal with 'attackers' who defeat security controls without their own knowledge? Most organizations feature some form of security action cycle that accounts for insider threat, and incorporate a risk driven approach proscribing the appropriate focus and tools, as well as investing in a balanced mix of technical controls and procedures. [132] It is rare to see a threat prediction model however, that also takes accidental threat into account. [133] This is important however, since the boundaries between trusted and un-trusted users within organizations have become much more blurred in this changing contemporary business world. It would be rewarding to see if the same fanatic deconstruction of malicious insider threats could also occur for the non – malicious or accidental side, where for example detection occurs timely enough within the process of a legitimate 'attack' and appropriate action is taken. [134]

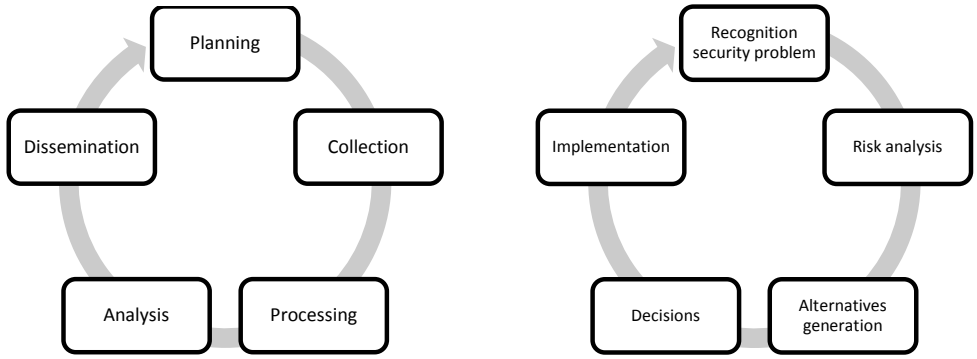
2.1.10 Processes and the security action cycle

Policy alone is therefore not the only solution. [135] Detection processes and containment are also currently key elements for controlling the insider threat, as they are effective for opportunistic and unethical intentions, and they also share their impact towards accidental incidents. The challenge to overcome is to provide effective preventative measures that do not disrupt the workflow and efficiency too much. [136] The effectiveness of cyber security is directly tied towards the cyber security processes, [137] as well as people and technology. [138] The processes should be aligned to the organizations risk tolerance and business goals. [139]

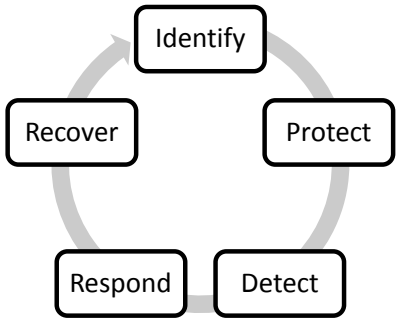
Processes can include for example incident response, security oversight, IT controls, management systems, governance frameworks, best practices, IT audits, and other different procedures. Processes make the implementation of an effective cyber security strategy happen by defining the organization's activities, roles, and documentation. [140] One viable strategy concerning processes is establishing a security action cycle, that aims to prevent, deter, detect, isolate, mitigate, or remedy threat or actions.[141] These action cycles are often based on

[131] D. Liu, X. F. Wang, J. Camp, *Game-theoretic modelling and analysis of insider threats,* International Journal of Critical Infrastructure Protection, 1, (2008), 75
[132] C. Colwill, *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009), 187
[133] G. B. Magklaras, S. M. Furnell, *Insider Threat Prediction Tool: Evaluating the probability of IT misuse,* in Computers & Security, 21(1), (2002), 62 – 73 ; P. A. H. Williams, *In a 'trusting' environment, everyone is responsible for information security,* in Information Security Technical Report, 13, (2008), 207
[134] D. Liu, X. F. Wang, J. Camp, *Game-theoretic modelling and analysis of insider threats,* in International Journal of Critical Infrastructure Protection, 1, (2008), 78
[135] P. A. H. Williams, *In a 'trusting' environment, everyone is responsible for information security,* in Information Security Technical Report, 13, (2008), 210
[136] P. A. H. Williams, *In a 'trusting' environment, everyone is responsible for information security,* in Information Security Technical Report, 13, (2008), 210
[137] https://www.itgovernance.co.uk/blog/organisations-failed-by-lack-of-cyber-security-processes/
[138] https://security-system.insuranceciooutlook.com/cxoinsights/people-processes-and-technology-mantra-for-cybersecurity-nid-190.html
[139] A. Chacko, *Cybersecurity – Integrating People, Process and Technology,* in IASA 87th annual educational conference & business show (2015), 10
[140] https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/
[141] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security 24, (2005), 474

'intelligence cycles', which are practices used for gathering intelligence and include aspects of planning, collection, processing, analysis, and dissemination in a continuous motion or cyclical pattern. [142] It should be noted however that in reality, there is often no strict cyclical pattern involved, and communication occurs both back and forth, as well as between tiers. [143] Security action cycles are derived , or at least inspired, of these intelligence cycles because of their proactive and reactive properties and nature in regards to information, as well as their feedback loop oriented methods and systems risk affiliation. [144]



Comparison of a basic intelligence cycle (left), a basic security action cycle (right) and a basic cyber security action cycle (below)



The above figure demonstrates a basic cyber security action cycle, which is inspired by the model of a basic intelligence cycle and a basic security action cycle. The basic model here is based upon the general cyber framework presented by the NIST (National Institute of Standards and Technology) of the US federal government in 2018. [145] It serves as basic format example and presents some of the basic functions that are in line with what

[142] L. K. Johnson, *Making the intelligence "cycle" work,* in International Journal of Intelligence and Counter Intelligence, 1(4), (1986) ; H. J. Davies, *The Intelligence Cycle is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine,* (2013), 1 - 23 accessed on https://bura.brunel.ac.uk/bitstream/2438/11901/3/Fulltext.pdf ; R. Willison, M. Warkentin, *The Expanded Security Action Cycle: A Temporal Analysis "Left of Bang",* in The Dewald Roode Information Security Workshop (Boston 2010), 397 – 398

[143] A. S. Hulnick, *What's wrong with the Intelligence Cycle,* in Intelligence and National Security, 21(6), (2006)

[144] D. W. Straub, R. J. Welke, *Coping With Systems Risk: Security Planning Models for Management Decision Making,* in MIS Quarterly, 22(4), (1998), 441 - 461

[145] https://www.nist.gov/cyberframework

information system security action cycles should feature: a means of deterrence, prevention, detection, and remedies. [146] Not wanting to thread too much into detail, as every cyber security specialist features their own version of an effective action cycle, [147] it can be rewarding to understand what is expected from the different components. [148] In general, identification and understanding of a cyber security risk or problem in relation to a system is at hand. Protection and measures to protect and maintain critical infrastructures and services is assured. Detection and identification processes ensure the observation of possible threats or events. Response consist of arrangements upon acting on detected threats or events. Finally, recovery and plans of restoration are in order to ensure the capabilities of services that would be, or have been, impaired.

Thus an action cycle that can prevent, detect, isolate and mitigate seems to be an appropriate solution. Knowledge of the end users is a must, and solid policy is the backbone of any organization attempting to deal with both malicious and accidental insider threat. Communication is key, and consistent, timely response towards incidents is an important matter. We have now explored the insider threat, but what about their underlying psychological reasoning? What about the influence of their behaviour? [149]

2.2 Contribution through criminology

True analysis of the motivation for betrayal requires complex psychological analysis and will vary from person to person. So how can we gain insight in the motivation of insiders? There are theories available that are already deeply established within the IS security field, especially within IS security management. These theories offer a more psychological contribution towards CIS problems and find their roots in criminology. While these theoretical approaches can sometimes be questioned for their effectiveness, [150] they are still regarded as being useful due to the need of a greater understanding of the relationship between actual actions of computer abuse and the organisational environment where such actions take place, all to enable more possible areas for safeguards. [151] The five largest theories used are: General Deterrence Theory (GDT), Social Bond Theory (SBT), Social

[146] D. B. Parker, *Fighting computer crime: a new framework for protecting information* (New York 1998), 310 – 347

[147] J. M. Stewart, *Cybersecurity Frameworks to Consider for Organization-wide Integration,* in Expert Reference Series of White Papers (2016), 2 – 8

[148] http://www.ignite.com.au/cyber-security-framework.html

[149] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, M. Whitty, *Understanding Insider Threat: A Framework for Characterising Attacks,* in 2014 IEEE Security and Privacy Workshops (San Jose 2014), 215 - 227 ; L. Hadlington, *The "Human Factor" in Cybersecurity: Exploring the Accidental Insider,* in J. McAlaney, L. A. Frumkin, V. Benson, *Psychological and Behavioral Examinations in Cyber Security* (2018), 46 – 61

[150] R .E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, R. Baskerville, *Future directions for behavioral information security research,* in Computers & Security 32, (2013), 92 ; M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24 (2005), 474

[151] R. Willison, *Understanding the offender/environment dynamic for computer crimes: assessing the feasibility of applying criminological theory to the IS security context,* in Proceedings of the 37th Hawaii international conference on system sciences (2004), 1

Learning Theory (SLT), Theory of Planned Behaviour (TPB), and Situational Crime Prevention (SCP). [152]

2.2.1 GDT (General Deterrence Theory)

General Deterrence Theory uses motive as a focal concept, with the base principal being logical decision making at the maximization of benefit in combination with the minimization of cost. [153] The person commits a crime if the expected benefit outweighs the cost of sanction. [154] The added value of GDT to IS security, through its focus on motive, is to tackle computer abuse before it actually happens. We have already shortly discussed one of its applications: the security action cycle, handling computer abuse through the four stages of deterrence, prevention, detection, and remedies. [155] Deterrence is achieved through policies, guidelines, and awareness programmes. Prevention is used when deterrence is ineffective and consist of physical and procedural controls. Detection aims at revealing the abuser, while remedies take effective action against the abuser or focus on restoration of information.

Academically, GDT is often used in conjunction with other behavioural models. This is because GDT has a tradition of providing hierarchical frameworks for security management, with an overreliance on technology and processes. [156] Implementation of anti – virus, systems, password protection, these mark general deterrence. This is usually supplemented with strict enforcement of security policies, as well as ensuring security awareness through security education. [157] Only as of recently has there been shown interest in combining GDT with organizational and behavioural perspectives or human interest. [158] One of such examples is a combination with SCT (Social Control Theory ; part of TPB which will be discussed more in depth later), which explains negative relationships between independent variables and dependent variables. This means that negative affects create pressure for corrective action,

[152] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24 (2005), 478

[153] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24 (2005), 474

[154] C. Beccaria, *On crime and punishments* (Indianapolis 1963) ; Q. Hu, Z. Xu, T. Divev, H. Ling, *Why Individuals Commit Computer Offences in Organizations: Investigating the Roles of Rational Choice, Self-Control, and Deterrence,* in Supply Chain and Information Management Conference Papers, Posters and Proceedings, 13, (2010), 1

[155] D. W. Straub, R. J. Welke, *Coping with systems risk: security planning models for management decision making,* in Management Information Systems Quarterly, 22(4), (1998), 446

[156] S. M. Lee, S. G. Lee, S. Yoo, *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004), 708 ; M. M. Eloff, S. H. von Solms, *Information security management: a hierarchical framework for various approaches,* in Computer and Security, 19(3), (2000), 243 – 256

[157] J. A. Hoffer, D. W. Straub, *The 9 to 5 underground: are you policing computer crimes?,* in Sloan Management Review, 30(4), (1989), 35 – 44 ; B. Bulgurcu, H. Cavusoglu, I. Benbasat, *Information Security Policy Compliance: An Empirical Study of Rationality – Based Beliefs and Information Security Awareness,* in MIS Quarterly, 34(3), (2010), 523 – 544

[158] G. Dhillon, J. Backhouse, *Information system security management in the new millennium,* in Communications of the ACM, 43(7), (2000), 125 – 128 ; M. Kuhalampi, *impact of deterrence theory methods on employees'' information security behavior* (Jyväskylä 2017), 6 – 26 ; J. D'Arcy, A. Hovav, D. Galletta, *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,* in Information Systems Research (2008), 1 – 16

leading insiders to abuse computers or IS processes and/ or policy in order to achieve a goal or attack / escape the source of their problem. [159] Ergo, negative effects can lead insiders to either self-defence (positive use of IS security), or induction control (negative use of IS security).

The most important aspect of GDT is not which precise model to use, but knowing that anticipating motive and adjusting behaviour accordingly through the means of deterrent techniques, [160] such as for example security policy, will most likely have a positive result on declining computer abuse. General deterrence factors seem to heavily affect insiders' abuse, even when the intention towards abuse is high. [161] It is yet confirmed by another study, that organizations featuring security countermeasures based off of GDT show a lower amount of computer abuse. [162] GDT is an applicable concept throughout various organizations. [163] In conclusion, there is no inherent doubt possible that GDT can be successfully applied to the IS environment, even when considering its roots within IS security lie on principles established in the late 1980's. [164]

2.2.2 SBT (Social Bond Theory)

Social Bond Theory also uses motive as a focal concept, with the base principle being a focus on the commitment of crime if social bonds of attachment, commitment, involvement, and belief are weak. [165] The theory seeks to explain social behaviour that does not conform to generally accepted social rules, based on the hypothesis that a natural inclination towards crime is supressed through strong social bonds. [166] Application of SBT to IS security has already been shortly discussed in the model presented by Lee, Lee, and Yoo (2004) as Social Control Theory, where attachment, commitment, involvement, and belief are explored as factors to organisational trust in order to reduce computer abuse. [167] Another interesting

[159] S. M. Lee, S. G. Lee, S. Yoo, *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004), 708 ; C. Beccaria, *On Crime and Punishment* (Indianapolis 1963) ; D. A. Smith, P. R. Garton, *Specifying specific deterrence,* in American Sociological Review, 54, (1989), 94 – 106

[160] D. W. Straub, R. J. Welke, *Coping with Systems Risk: Security Planning Models for Management Decision Making,* in Management Information Systems Quarterly, 22(4), (1998), 445

[161] S. M. Lee, S. G. Lee, S. Yoo, *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004), 715 – 716

[162] D. W. Straub, *Effective IS Security: An Empirical Study,* in Information Systems Research, 1(3), (1990), 255

[163] J. H. Schuessler, *General Deterrence Theory: Assessing Information Systems Security Effectiveness In Large Versus Small Businesses,* in Dissertation for the Degree of Doctor of Philosophy (University of North Texas 2009), 41 – 69

[164] P. Gray, W. King, E. McLean, H. Watson (eds.), J. A. Hoffer, D. W. Straub, *The 9 to 5 Underground: Are You Policing Computer Crimes?,* in Management of Information Systems (1994), 388 ; J.A. Hoffer, D.W. Straub, *The 9 to 5 Underground: Are You Policing Computer Crimes?,* in Sloan Management Review, 30(4), (1989), 35 ; D. W. Straub, *Effective IS Security: An Empirical Study,* in Information Systems Research, 1(3), (1990), 255 ; D. W. Straub, W. D. Nance, *Discovering and Disciplining Computer Abuse in Organizations: A Field Study,* in Management Information Systems Quarterly, 14(1), (1990), 45

[165] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 478

[166] T. Hirschi, *Causes of Delinquency* (Berkeley 1969), 3 – 15

[167] S. M. Lee, S. G. Lee, S. Yoo, *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004), 708 – 710

approach towards using SBT in IS security is by considering both formal and informal control factors, presented in an integrated model together with existing deterrence theory. [168] It is argued then, that social bonds and social pressures may act as informal controls. [169] These informal controls are social customs, traditions, norms, morality or other values and are implemented by unofficial controlling groups or individuals. [170]

The predicament is that someone who is strongly bonded to conventional society, the less likely it is that this person will deviate from conventional norms and participate in delinquent behaviour. Having a good or strong bond with an immediate supervisor for example can decrease the likeliness of an employee engaging in deviant behaviour. [171] Different attitudes of individuals towards their jobs can having different implications towards possible delinquent behaviour. Someone who is very attached to their organizations, who perhaps shares a deep affection towards it, is probably more inclined to care about the safeguard of their organization than someone who is merely in there 'for the money'. [172] It is argued, hypothesized, and even confirmed that these committed individuals are less inclined to violate security policy, especially because they seek to improve their own position conform to the organization's standards. [173] Of course, we have to remain critical here as study has also shown that information system security policy is not always complied with, even by people who are strongly bonded to their organization. [174]

Apart from the attachment, commitment and involvement towards the organization and its society, another important factor of SBT is 'belief', or personal norms. [175] How individuals perceive their actions and the attitude they hold towards non-compliant security behaviour appears to hold heavy influence on performing the actual deed. [176] When these beliefs in social values are absent or weak, the possibility of a person engaging in antisocial acts increase. [177] Beliefs are heavily subjective however and can be influenced by a multitude of

[168] L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013), 447
[169] L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013), 448
[170] S. Jiang, E. Lambert, M. Jenkins, *East meets West: Chinese and U.S. college students' views on formal and informal crime control,* in International Journal of Offender Therapy and Comparative Criminology, 54(2), (2010), 264
[171] Q. Zhai, M. Lindorff, B. Cooper, *Workplace guanxi: its dispositional antecedents and mediating role in the affectivity – job satisfaction relationship*, in Journal of Business Ethics, 117(3), (2013), 550
[172] L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013), 451
[173] L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013), 452, 455
[174] P. Ifinedo, *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,* in Information & Management, 51, (2014), 69 ; A. Vance, M. Siponen, S. Pahnila, *Motivating IS security compliance: insights from habit and protection motivation theory,* in Information & Management, 49(3), (2012), 190
[175] P. Ifinedo, *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,* in Information & Management, 51, (2014), 70
[176] A. Peace, D. Galleta, J. Thong, *Software piracy in the workplace: A model and empirical test,* in Journal of Management Information Systems, 20(1), (2003), 169
[177] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24 (2005), 475

factors, such as environment, norms, and individual characteristics,[178] as well as shift over time. [179] Social pressure seems to be able to influence attitude [180] in some cases with regard to ISSP compliance behaviour. [181] Co – worker behaviour seems to be able to exert social pressure, [182] as well as the own subjective norm, which is the perceived social pressure to perform or not perform a certain behaviour. [183]

It appears that SBT is genuinely attractive to incorporate in any information security assessment, but it could be considered more difficult than GDT due to its more subjective nature. Nonetheless, it is extremely relevant towards any modern information security agenda and could definitely be incorporated in an analytical assessment. Being able to detect an attack before it happens could be enhanced through detecting and/or elimination motivation beforehand.

2.2.3 SLT (Social Learning Theory)

Social Learning Theory uses motive as a focal concept, with the base principle being a focus on the commitment of a crime if that person associates with delinquent peers, who transmit delinquent ideas, reinforce delinquency and function as delinquent role models. [184] The theory is a combination of differential association and differential reinforcement / punishment. The former is the process during which a person is exposed to normative definitions that either favour or appal criminal behaviour, [185] essentially meaning that criminal behaviour is learned through interaction with others in a process of communication. [186] The latter refers to the idea of expected and/or realized reward and punishment, resulting from criminal behaviour, [187] essentially meaning that criminal behaviour is learned through a process of expectations conform behaviour. Definitions of behaviour and imitation are also two major concepts within this theory. [188] Definitions of behaviour are the attitudes about certain behaviour learned through the process of association, imitation and interaction or

[178] T. Cronan, C. Foltz, T. Jones, *Piracy, computer crime, and IS misuse at the university,* in Communications of the ACM, 49(6), (2006), 84
[179] L. Leonard, T. Cronan, *Attitude toward ethical behavior in computer use: a shifting model,* in Industrial Management + Data Systems, 105(9), (2005), 1150
[180] A. Rivis, P. Sheeran, *Descriptive norms as an additional predictor in the theory of planned behaviour: a meta-analysis,* in Current Psychology, 22(3), 2003, 218
[181] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24 (2005), 452
[182] T. Herath, H. R. Rao, *Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness,* in Decision Support Systems, 47(2), (2009), 155 – 158
[183] V. Venkatesh, S.A. Brown, *A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges,* in Management Information Systems Quarterly, (2001), 73
[184] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24 (2005), 478
[185] E.H. Sutherland, *Principles of criminology* (Chicago 1947), 6-7 ; D.R. Cressey, *The Theory of Differential Association: an Introduction,* in Social Problems, 8(1), (1960), 2
[186] E.H. Sutherland, D.R. Cressey, *A Theory of Differential Association,* in F. T. Cullen, R. Agnew (eds), *Criminological Theory: Past to Present* (Los Angeles 2006), 122 – 125
[187] R. L. Burgess, R. L. Akers, *A Differential Association-Reinforcement Theory of Criminal Behavior,* in Social Problems, 14(2), (1966), 134, 143
[188] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24 (2005), 456

exposure to sources of learning in a certain social environment; they are the moral attitude that define an act as 'good' or 'bad'. [189] Imitation is the modelling of certain behaviour through the observation of others and/or the behaviour of others. [190]

The primary point here is the social surrounding and the impact it has on an individual, with regard to engaging in criminal behaviour. Friend's involvement and perceived certainty of being caught are two variables for example that have been found to strongly correlate with computer crime, [191] as well as general group trends that persist towards the individual. [192] Differential reinforcement and punishment, as well as sources of imitation appear to be significantly related to computer crime. [193] Other studies find that the social environment can definitely affect 'media – related attitudes or behaviour in organizations', [194] as well as their security behaviour, [195] going as far as to state that choices under conditions of objective rationality can still be subjected to social influences. [196]

So can SLT be successfully applied to an analytical assessment? Taking the social environment and possible influences that it can have on the behaviour of the individual will most certainly be beneficial. SLT has already been applied to some older, [197] and some more modern models in information security, [198] leading to a relatively well established approach

[189] R. L. Akers, *Criminological Theories: Introduction and Evaluation* (Los Angeles 1994), 97
[190] W. F. Skinner, A. M. Fream, *A Social Learning Theory Analysis of Computer Crime Among College Students,* in Journal of Research in Crime and Delinquency, 34(4), (1997), 499
[191] R. C. Hollinger, *Crime by computer: correlates of software piracy and unauthorized account access,* in Security Journal, 2(1), (1992), 2 – 12
[192] W. D. Gunter, G. E. Higgins, R. E. Gealt, *Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents,* in International Journal of Cyber Criminology, 4(1-2), (2010), 668
[193] W. F. Skinner, A. M. Fream, *A Social Learning Theory Analysis of Computer Crime Among College Students,* in Journal of Research in Crime and Delinquency, 34(4), (1997), 496
[194] J. Fulk, C. W. Steinfield, J. Schmitz, J. G. Power, *A Social Information Processing Model of Media Use in Organizations,* in Communication Research, 14(5), (1987), 530
[195] K. Parsons, A. McCormac, M. Butavicius, L. Ferguson, *Human Factors and Information Security: Individual Culture and Security Environment,* in Command, Control, Communications and Intelligence Division DSTO-TR-2484 (2010), 11
[196] J. Fulk, C. W. Steinfield, J. Schmitz, J. G. Power, *A Social Information Processing Model of Media Use in Organizations,* in Communication Research, 14(5), (1987), 538
[197] R. L. Akers, *Deviant Behavior: A Social Learning Approach* (California 1985), 39 ; R. Agnew, *Testing the leading crime theories: an alternative strategy focusing on motivational process,* in Journal of Research in Crime and Delinquency, 32(4), (1995), 374 – 376, 381 ; C.R. Tittle, M. J. Burke, E. F. Jackson, *Modeling Sutherland's theory of differential association: toward an empirical clarification,* in Social Forces, 65, (1986), 412, 429 ; M.D. Krohn, W. F. Skinner, J.L. Massey, R. L. Akers, *Social learning theory and adolescent cigarette smoking: a longitudinal study,* in Social Problems, 32(5), (1985), 455 – 460, 462, 464, 468 – 469 ; W. F. Skinner, A. M. Fream, *A social learning theory analysis of computer abuse among college students,* in Journal of Research in Crime and Delinquency, 34(4) (1997), 509 – 510, 512 – 514
[198] J. Lee, Y. Lee, *A holistic model of computer abuse within organizations,* in Information Management & Computer Security, 10(2), (2002), 60 – 61 ; T .J. Holt, G. W. Burruss, A. M. Bossler, *Social learning and cyber deviance: examining the importance of a full social learning model in the virtual world,* in Journal of Crime & Justice, 33(2), (2010), 32 – 38 ; G .E. Higgins, *Gender Differences in Software Piracy: the Mediating Roles of Self-control Theory and Social Learning Theory,* in Journal of Economic Crime Management, 4(1), (2006), 7 – 10, 18 – 20

that is undeniably important in explaining important social structural factors that influence criminal behaviour. [199]

2.2.4 TPB (Theory of Planned Behaviour)

The Theory of Planned Behaviour uses motive as a focal concept, with the base principle being a focus on the intention towards crime that a person can have as a factor in predicting behaviour. [200] As a theory that seeks to explain the causal relation that underlies human behaviour, the basic assumption is that intention is a key factor for predicting a person's behaviour. [201]

The background of this theory stems from the 'theory of reasoned action', which supposes a causal sequence from beliefs to behaviour through attitude, social norms and intention. [202] Behaviour is thus seen as a function of behavioural intentions that are in turn a function of attitudes, subjective norms, and perceived behavioural control. [203] Attitudes refer to the degree to which the person has a favourable or unfavourable evaluation of the behaviour in question. [204] These attitudes, also known within the theory as 'behavioural beliefs', thus shape the link between the behaviour of interest towards an expected outcome. [205] Subjective norms, also known as perceived behavioural control, refers to perceived social pressure. [206] This perception of social pressure helps as a second determinant of intention to perform the behaviour under consideration. [207] This means that a person can be motivated to comply with social demands, resulting in either positive or negative behaviour , depending on the current social norm. [208] Perceived behavioural control refers to the sense of self-efficacy, or ability to perform the behaviour of interest. [209] If people are realistic in their judgement of the feasibility of a certain behaviour the measure of perceived behavioural control can serve as a

[199] T. J. Holt, G. W. Burruss, A .M. Bossler, *Social learning and cyber deviance: examining the importance of a full social learning model in the virtual world,* in Journal of Crime & Justice, 33(2), (2010), 35
[200] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 478
[201] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 478
[202] V. T. Sarver JR. *Ajzen and Fishbein's "Theory of Reasoned Action": A Critical Assessment,* in Journal for the Theory of Social Behaviour, 13(2), (1983), 1 ; T. J. Madden, P. Scholder, E. I. Ajzen, *A comparison of the Theory of Planned Behavior and the Theory of Reasoned Action,* in Personality and Social Psychology Bulletin, 18(1), (1992), 3 – 9
[203] C. Nisson, A. Earl, *The Theories of Reasoned Action and Planned Behavior: Examining the Reasoned Action Approach to Prediction and Change of Health Behaviors,* in K. Sweeny, M. Robbins (eds.) *The Wiley Encyclopedia of Health Psychology* (2017), 1 – 2
[204] J. Lee, Y. Lee, *A holistic model of computer abuse within organizations,* in Information Management & Computer Security, 10(2), (2002), 58
[205] http://people.umass.edu/aizen/bb.html ; I. Ajzen, *Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior,* in Journal of Applied Social Psychology, 32(4), (2002), 665
[206] I. Ajzen, *Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior,* in Journal of Applied Social Psychology, 32(4), (2002), 665
[207] I. Ajzen, *Attitudes, Personality and Behavior* (New York 2005), 118
[208] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 478
[209] I. Ajzen, *Attitudes, Personality and Behavior* (New York 2005), 118

proxy for actual control and contribute towards the prediction of the behaviour in question. [210] A person thus shapes intention based on personal beliefs, concerning the difficulty of realizing this behaviour and the ability in successfully carrying it out, resulting in behaviour occurring if the person has a strong perceived control over it. [211]

The concept of behavioural control appears to derive from three previous concepts. [212] At first, the concept of health believe model , [213] presents the argument of barriers that may or may not prevent action being taken. Though originally used to measure the readiness to use health services, [214] the concept of mental and physical barriers of some sort is extremely relevant towards any IS security analysis. The second concept, interpersonal behaviour, [215] was at first developed as an alternative towards the theory of reasoned action (TRA) and the theory of planned behaviour (TPB) ; before the addition of behavioural control. [216] Recognizing the key roles played by social factors and emotions forming intentions, but also the importance of past behaviour on the present, [217] intentions are seen as immediate antecedents of behaviour, but habits also mediate behaviour, which are both moderated by facilitating conditions. [218] These facilitating conditions, which eventually lead to behavioural control within TPB, are conditions that either enable or hinder the performance of particular behaviour. [219] Important to note is that within the original TPB, behaviour was a direct function of intention while TIB (theory of interpersonal behaviour) suggested that the facilitating conditions as well as intention and habits are a direct influence towards behaviour.

We have now seen that perceived behavioural control can directly influence both intention, as well as the behaviour in question. Knowing which factors possibly influence behaviour is a great addition towards an analytical framework for assessing information security, in both their predictive, anticipating and explanatory nature. The third concept is that of perceived self – efficacy. This concept refers to people's beliefs about their capabilities to exercise control over their own level of functioning, and over events that affect their lives. [220] Behaviour is broken down into its successive elements, and self – efficacy is analysed in

---

[210] C.J. Armitage, M. Conner, *Efficacy of the theory of planned behavior: A meta-analytic review,* in British Journal of Social Psychology, 40, (2001), 485 – 489

[211] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 476

[212] I. Ajzen, *Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior,* in Journal of Applied Social Psychology, 32(4), (2002), 667

[213] I. M. Rosenstock, *Why people use health services,* in Milbank Memorial Fund Quarterly, 44, (1966), 100 – 102

[214] I. M. Rosenstock, *Why people use health services,* in Milbank Memorial Fund Quarterly, 83(4), (2005), 9 – 14

[215] H. C. Triandis, *Interpersonal behaviour* (California 1977) ; J. Robinson, *Triandis' theory of interpersonal behaviour in understanding software piracy behaviour in the South African context,* Doctoral dissertation (February 2010), 12 – 33

[216] G. D. Moody, M. Siponen, *Using the theory of interpersonal behaviour to explain non-work related personal use of the Internat at work,* in Information & Management, 50, (2013), 325

[217] http://www.cres.gr/behave/pdf/Triandis_theory.pdf

[218] http://www.cres.gr/behave/pdf/Triandis_theory.pdf

[219] R. R. Milhausen, M. Reece, B. Perera, *A theory – based approach to understanding sexual behaviour at Mardi Grass,* in the Journal of Sex Research, 43, (2006), 97 – 107

[220] A. Bandura, *Social cognitive theory of self – regulation,* in Organizational Behavior and Human Decision Processes, 50, (1991) ,257

terms of perceived ability to perform each step in the chain, under a variety of circumstances. [221] We are interested in the way people are able to perform a particular behaviour, instead of their perceived control over events or outcomes though. Luckily, it is explained that efficacy expectation means a conviction that a person can successfully execute the behaviour required to get a certain outcome, and that self – efficacy refers to the beliefs in one's capabilities to think out and execute courses of action required to achieve a goal to which that person is working. [222] The greatest addition towards perceived behavioural control is then the fact that both concern themselves with the perceived, subjective, ability to perform a behaviour, which can both directly influence both the intention and the outcome, without being mutually exclusive. This leads to perceived behavioural control to be readable as "perceived control over performance of a behaviour", [223] allowing it to be measured in an information security environment by asking direct questions about capability to perform a behaviour, or appealing towards the basis of beliefs about being able to perform a certain behaviour.

Returning back to the three factors: attitudes, subjective norms, and perceived behavioural control, these eventually lead to actual behavioural intention. When given a sufficient degree of actual control over their behaviour, people are expected to carry out their intentions when the opportunity arises, or when they have the means to do so, [224] leaving intention as the immediate antecedent of behaviour. [225] It is important to note that the theory assumes the relative importance of either of the three options. This means that sometimes normative considerations are for example more important than the behavioural beliefs. Thus in some instances only one, two, or all three factors are needed to explain the intention. The relative weight of the three factors can vary per individual and can depend on other factors within the social environment. [226]

Another important aspect is the fact that this theory does not deal directly with the amount of control a person actually has in a given situation, but considers the possible effects of perceived control. Intentions reflect a certain willingness to enact a certain behaviour, and perceived control takes realistic constraints into account. [227] The three factors are therefore not mutually exclusive and do not guarantee the result of a certain behaviour. Vice versa, behaviour might also occur without a certain intention. A valid question thus arises: when measuring all of these cognitive variables to predict behaviour, how can we validate their

[221] I. Ajzen, *Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior,* in Journal of Applied Social Psychology, 32(4), (2002), 667 – 668
[222] A. Bandura, *Health promotion from the perspective of social cognitive theory,* in Psychology and Health, 13, (1998), 624
[223] I. Ajzen, *Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior,* in Journal of Applied Social Psychology, 32(4), (2002), 668
[224] I. Ajzen, *Attitudes, Personality and Behavior* (New York 2005), 118
[225] I. Ajzen, *Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior,* in Journal of Applied Social Psychology, 32(4), (2002), 665 ; M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 478
[226] I. Ajzen, *Attitudes, Personality and Behavior* (New York 2005), 118
[227] I. Ajzen, *Attitudes, Personality and Behavior* (New York 2005), 118 – 199

conclusions? [228] The answer is rather ambiguous. This should indeed be taken into account when predicting behaviour, as well as when we seek to explain behaviour. Validation of these cognitive variables is not the primary goal, but to better understand the phenomenon of computer abuse these causal variables can be considered. [229] Success in explaining behaviour and righteously predicting abuse and thus being able to deter it successfully through these variables is then validation.

Possibilities to combine this theory with computer abuse have been, successfully, explored. [230] Interestingly enough, a major take in these studies is that GDT, SBT and SLT can be combined with TPB, resulting in the knowledge that social bonds can affect the behavioural beliefs (or attitudes), social learning can affect the subjective norms, and general deterrence can form perceived behavioural control. [231] As the human factor remains both the weakest link and the area where major improvements towards information security are to be made, understanding behaviour in an analytical way is a must, especially when considering improving user security behaviour, which is tied to their understanding of what behaviour is expected and their willingness to comply with these accepted norms. [232]

2.2.5 SCP (Situational Crime Prevention)

The theory of Situational Crime Prevention uses opportunity as a focal concept, with the base principle being a focus on the occurrence of crime when there is both motive and opportunity, reasoning crime is reduced when no opportunities exist. [233] As a theory, the main hypothesis is that a person must have both motive and opportunity to commit a crime. [234] With the main focus on crime prevention being on motive, resulting in 'social crime prevention', it appeared that situational measures were being devalued. [235] The idea of crime being opportunity, [236] and situational based, [237] was then initially met with some resistance

[228] J. Holdershaw, P. Gendall, *Understanding and predicting human behaviour,* in ANZCA08 Conference, Power and Place, Wellington, (July 2008), 2 – 11
[229] J. Lee, Y. Lee, *A holistic model of computer abuse within organizations,* in Information Management & Computer Security, 10(2), (2002), 58
[230] C. L. Anderson, R. H. Smith, *Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions,* in Management Information Systems Quarterly, 34(3), (2010), A1-A3 ; F. D. Davis, *User acceptance of information technology: system characteristics, user perceptions and behavioral impacts,* in International Journal of Man-Machine studies, 38(3), (1993), 1 – 13 G. D. Moody, M. Siponen, *Using the theory of interpersonal behavior to explain non – work related personal use of the Internet at work,* in Information & Management, 50, (2013), 322 – 335
[231] J. Lee, Y. Lee, *A holistic model of computer abuse within organizations,* in Information Management & Computer Security, 10(2), (2002), 57 – 60
[232] J. Leach, *Improving user security behaviour,* in Computers and Security, 22(8), (2003), 685 – 692
[233] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 478
[234] R. V. G. Clarke, *Situational Crime Prevention: Theory and Practice,* in the British Journal of Criminology, 20(2), (1980), 138, 140 – 141
[235] R. V. G. Clarke, *Situational Crime Prevention: Theory and Practice,* in the British Journal of Criminology, 20(2), (1980), 145
[236] P. Mayhew, R .V. G. Clarke, A. Sturman, J. M. Hough, *Crime as Opportunity,* in Home Office Research Study no. 34 (London 1976), 3, 29 – 30 ; N. Morris, G. Hawkins, *The Honest Politician's Guide to Crime Control* (Chicago 1970),

, [238] as well as praise, [239] but seems to have evolved into a generally well established theory within the contemporary field. [240]

The theory appears to be based on the principles of routine activity theory and rational choice theory. [241] Routine activity theory looks at the characteristics of the crime instead of the person committing it. [242] Instead of centring on psychological, biological, or social factors that motivate a criminal act, this theory regards crime as an event, highlighting the relation to space, time, and approaching it through an ecological way. [243] Through this approach, criminal acts appear to require a convergence in space and time of likely offenders, suitable targets, and the absence of capable guardians against crime. [244] The structure of routine activities within a society can influence what kind of situations occur, and people act in response to these situations. [245] Therefore, situations encountered can influence the crime involvement of citizens of this society. This theory is mainly used to explain a rise in crime in societies that seem prosperous and lacking of otherwise crime inducing traits, such as for example poverty. [246] Rational choice theory within criminology tries to explain crime from the perspective of the offender, focusing on the thinking and decision making process of an offender, looking at criminal opportunities and how the decision to commit a crime is reached. [247] The theory is often used to provide insight in 'choice – structuring properties', which provide a constellation of opportunities, costs and benefits attached to a particular kind

---

[237] P. Mayhew, R. V. G. Clarke, A. Sturman, J. M. Hough, *Crime as Opportunity,* in Home Office Research Study no. 34 (London 1976), 1 – 2

[238] C. D. Breitel, *Reviews,* in The University of Chicago Law Review 37, (1970), 633 ; L. Radzinowicz, J. King, *The Growth of Crime* (London 1977) ; R. V. G. Clarke, *Situational Crime Prevention: Theory and Practice,* in the British Journal of Criminology, 20(2), (1980), 145

[239] E. L. Barrett Jr., *Book reviews,* in Southern California Law Review, 44(2), (1971), 517 - 523

[240] J. D. Freilich, G. R. Newman, *Situational Crime Prevention,* in Oxford Research Encyclopedia of Criminology (Oxford 2018), 2 ; R. V. Clarke, *Theoretical Background to Crime Prevention through Environmental Design (CPTED) and Situational Prevention,* in Paper presented at the Designing Out Crime: CPTED convened by the AIC and NRMA Insurance, Hilton Hotel (Sydney 1989), 2 – 8 ; M. Felson, R. V. Clarke, *Opportunity Makes the Thief Practical theory for crime prevention,* in Police Research Series Paper 98 (London 1998), v – vi ; R. V. Clarke, *Opportunity makes the thief. Really? And so what?,* in Crime Science, 1(3), (2012), 1 ; I. Waller, *Preventing property crime in communities, by communities,* in Smarter Crime Control, a Guide to a Safer Future for Citizens, Communities, and Politicians (Plymouth 2014), 206 – 207

[241] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 477 ; J. D. Freilich, G. R. Newman, *Situational Crime Prevention,* in Oxford Research Encyclopedia of Criminology (Oxford 2018), 1

[242] R. V. Clarke, *Situational crime prevention: theory and practice,* in British Journal of Criminology, 20, (1980), 136 – 137 ; L. E. Cohen, M. Felson, *Social change and crime rate trends: a routine activity approach,* in American Sociological Review, 44, (1979), 588 – 590

[243] F. Miró, *Routine Activity Theory,* in J. M. Miller (ed.), The Encyclopedia of Theoretical Criminology (New Jersey), 1

[244] L. E. Cohen, M. Felson, *Social change and crime rate trends: a routine activity approach,* in American Sociological Review, 44, (1979), 588, 604 – 605

[245] H. Wikström, *Routine Activity Theories,* in Oxford Bibliographies Online, (2016) accessed on http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0010.xml

[246] F. Miró, *Routine Activity Theory,* in J. M. Miller (ed.), The Encyclopedia of Theoretical Criminology (New Jersey), 1

[247] D. Cornish, R. Clarke, *Introduction*, in D.B. Cornish, R. V. Clarke (eds.), The Reasoning Criminal (New Jersey 2014), 1 – 6

of crime. [248] The rational choice perspective on crime assumes that offenders somehow seek to benefit themselves by their criminal act (or behaviour), using cognitive abilities and available relevant information which is eventually lead by the making of decisions and choices with some form of rationality. [249]

When looking at rational choice theory, in essence relying on the utilitarian fact that man can rationally make their own decisions, it is important to not get lost in an endless debate versus theories that claim otherwise, such as for example theories that feature uncertainty, institutions, structuralism, socioeconomic environment or determination. [250] What is important, is that we can use the insights rational choice theory provides us, combined with routine activity theory insights to use the SCP and look at opportunity instead of motive. I do not believe these other theories cannot provide the same, or alternative insights, but rational choice theory has already proven itself within the criminology field to be a great asset in the explanatory and preventive value it brings. [251] On top of this, one issue that is not often present within the discussion of this theory, but seems extremely relevant to me, is that of accountability. A rational actor suggests that he is accountable for his own actions. Who is responsible for a crime if the actor did not make a rational decision? Though this seems like a matter for criminal justice, I deem it a relevant argument in considering the value rational choice theory brings and the way it influences SCP, also validating its usefulness.

So far, with the combined concepts of the above theories, we can see that the theory of SCP aims to the undertaking of measures that will reduce criminal opportunities in a certain context or place where criminal actions take place. [252] Implementation of opportunity reducing techniques can impact their environment through its design, management, or manipulation, and aim to either increase the effort and risks of crime, render crime less rewarding or excusable, or reduce provocative phenomena in the immediate context. [253] Safeguards are usually introduced in the immediate environment, their purpose being an impact to the offender's perception of potential cost and benefits of committing a crime. [254] Interestingly enough, SCP seems to also recognize moral costs during the decision making process, which perpetrators of criminal behaviour might try to supress or nullify through the construction of excuses. It would seem then, that environment also plays a major role

[248] D.B. Cornish, R. V. Clarke, *Understanding crime displacement: an application of rational choice theory*, in Criminology, 25(4), (1987), 933
[249] D.B. Cornish, R. V. Clarke, *Understanding crime displacement: an application of rational choice theory*, in Criminology, 25(4), (1987), 933, 935
[250] F. Huerga, *The Economic Behavior of Human Beings: The Instutitionalist/Post-Keynesian Model,* in Journal of Economic Issues, 42(3), (2008), 709
[251] J. Eck, D. L. Weisburd, *Crime Places in Crime Theory,* in Crime and Place: Crime Prevention Studies, 4, (2015), 1 ; R. V. Clarke, D. Weisburd, *Diffiusion of crime control benefits: observations on the reverse of displacement* (New Jersey), 1, 15 ; R. V. Clarke, M. Felson, (eds.), *routine activity and rational choice, advances in criminological theory volume 5* (New Jersey 2008), 1 – 17, 323 – 383
[252] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security, 24, (2005), 477
[253] R. Willison, M. Siponen, *Overcoming the insider: reducing employee computer crime through Situational Crime Prevention*, in communications of the ACM, 52(9), (2009), 134
[254] R. Willison, M. Siponen, *Overcoming the insider: reducing employee computer crime through Situational Crime Prevention*, in communications of the ACM, 52(9), (2009), 134

throughout the criminal though process, as a means to facilitate opportunity, according to SCP. [255]

The SCP theory has been applied throughout frameworks and models used towards improving many contemporary IS security policies. [256] It turns out to be a theory especially popular in reducing the insider threat due to the way it addresses motivation and opportunity. [257] Knowing SCP is often used in conjunction with other criminological theories in most of these cases, the benefits of applying SCP in our own analysis is rather self-explanatory. It has proven to provide a reliable model, also when paired with other criminology theories. Secondly, being such a well-established theory for decades within the criminology field, as well as currently within the IS security field, the unique focus it brings toward opportunity, situational variables and (social) environment in general is a great contribution towards any work that considers behavioural theories within IS security, since most of them focus on motive.

2.3 Security compliance theory

2.3.1 Downsides to behavioural theories?

Are there any downsides towards using these proposed theories? So far, most of these studies are related to cases of intellectual property theft, [258] or deviant behaviour in general. The criminology theories look to explain and/or predict deviant behaviour, labelling it as criminal. We have seen how all theories translate well and are most of the time already established within the IS security field. We have seen how motive and opportunity can influence and

[255] R. Hunter, R.C. Jeffrey, *preventing convenience store robbery through environmental design,* in R. Clarke (ed.), Situational Crime Prevention: successful case studies (New York 1997) ; J.E. Eck, *Preventing Crime at Places,* in L. Sherman, D. Gottfredson, D. Mackenzie, J. Eck, P. Reuter, S. Bushway (eds.), *Preventing Crime: What Works, What Doesn't, What's Promising* (Washington 1998), 43 – 50

[256] N. L. Beebe, V. S. Rao, *Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security*, in Proceedings of the 2005 SoftWars Conference, Las Vegas, NV, (December 2005), 1 – 18 ; N. L. Beebe, V. S. Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process,* in Communications of the Association for Information Systems, 26(17), (2010), 330 – 358 ; S. Hinduja, B. Kooi, *Curtailing cyber and information security vulnerabilities through situational crime prevention,* in Security Journal, 26(4), (2013), 383 – 402 ; H.G. Kim, *Development of the Dynamic Optimal Control Model for Information Security Strategy Choice to Maximize Information Security Compliance Intention,* in Korean Review of Corporation Management, 9(1), (2018), 19 – 30 ; D. Maimon, O.B. Malaya, R. Cathey, S. Hinton, *Re-thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors for Predicting Cyber Attacks,* in 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), (6-10 November 2017), 232 – 238 ; K. Padayachee, *An assessment of opportunity – reducing techniques in information security: An insider threat perspective,* in Decision Support Systems, 92, (2016)

[257] N. S. Safa, C. Maple, T. Watson, R. V. Solms, *Motivation and opportunity based model to reduce information security insider threats in organisations,* in Journal of Information Security and Applications, 1(11), (2017), 1 – 10 ; E.K. Stones, *Mobile Communications: M – Crime and Security,* in Ph.D in Security and Crime Science, University College London Department of Security and Crime Science (June 2017), 4, 88 – 101

[258] J.S. Albanese, *Intellectual Property and White-collar Crime: Report of Issues, Trends, and Problems for Future Research,* in J.S. Albanese (ed.), *Intellectual Property Theft and Fraud: Combating Piracy* (New York 2007), 73 – 95

forge criminal behaviour. But is this a fool proof way of predicting criminal behaviour? None of the criminology theories applied give a decisive judgement on whether an individual is actually going to perform a criminal act. While being strong in their predictive and explanatory power, we can still see how individuals who are given motive and opportunity do not reside to deviant behaviour, while those who lack both motive and opportunity might still do so. On top of that, how do we expect to measure these kind of behaviours and their influences exactly?

2.3.2 Security policy compliance

Most of the criminology models presented work in conjunction to security policy compliance theory. Failing to comply or successfully complying to ISSP (Information System Security Policy) accounts for more than just criminology theories. [259] This body of literature presents information security policy compliance (ISP), which is one of the key concerns in organizations dealing with information and data. [260] Organizations develop information systems security (ISS), and policies (ISSP), in order to achieve information assurance, which is defined as "the reliability, accuracy, security, and availability of a company's information assets… defin[ition of] how these assets – data and/ or information both within the tangible and the virtual bounds of the organization – should be secured to provide maximum benefit". [261] These procedural measures offer an alternative to technical defences, but by no means substitute the need for all human and/ or social factors, probably representing organizational factors more. [262]

ISSP's are in place then, to ensure employee compliance with security measures. Failure of employees to adhere to their organizations' security policies count as a key threat. [263] Surprisingly, study has shown that deterrence factors have a significant influence towards compliance rather than rewards. [264] It could be argued then, that models based on predicting / explaining deviant behaviour and assessing security compliance will yield better results than for example models focusing on rewarding good behaviour. The fundamentals of information security policy compliance help us better understand how theory and practice work together.

2.3.3 Risk management

[259] M. Siponen, S. Pahnila, M. A. Mahmood, *Compliance with Information Security Policies: An Empirical Investigation,* in Computer, 43(2), (2010), 1
[260] A.A. Omari, J. Walters, A. Deokar, H. Aleassa, O.E. Gayar, *Information Security Policy Compliance: An Empirical Study of Ethical Ideology,* in 46th Hawaii International Conference on System Sciences, (2016), 3018
[261] M.I. Merhi, P. Ahluwalia, *Information Security Policies Compliance: The Role of Organizational Punishment,* in Proceedings of the 19th Americas Conference on Information Systems, Chicago, Illinois, (15 – 17 August 2013), 1
[262] A.A. Omari, J. Walters, A. Deokar, H. Aleassa, O.E. Gayar, *Information Security Policy Compliance: An Empirical Study of Ethical Ideology,* in 46th Hawaii International Conference on System Sciences, (2016), 3018 – 3020
[263] M. Siponen, S. Pahnila, M. A. Mahmood, *Compliance with information security policies: an empirical investigation,* in Computer (2010), 64
[264] M. Siponen, S. Pahnila, M. A. Mahmood, *Compliance with information security policies: an empirical investigation,* in Computer (2010), 67

At first it is good to consider that many contemporary security strategies approaches feature a 'risk management' approach. [265] This begins with the identification of assets, threats, and vulnerabilities, after which a risk assessment takes place, where countermeasures are considered. [266] The purpose of risk management is to minimize expected loss. [267] Most organizations determine their cyber defences through a model that enables decision makers to perceive the amount of risk involved with certain aspects and choosing to spend budget accordingly to the amount of potential loss involved. This often means that unless a threat carries a severe risk implication, they remain unconsidered. Below is an example of a basic risk management model.

Impact	**Risk management options**		
High	Intensive management required	Manage & monitor risks	Extensive management essential
Medium	Accept risk with monitoring	Effort to manage is worthwhile	Management effort required
Low	Accept risks	Accept risk but monitor them as well	Manage and monitor risk
	Low	*Medium*	*High*
	Likelihood		

The countermeasures often include at least three types of strategy. [268] The first is target hardening trough technical countermeasures, such as for example using passwords, antivirus

[265] N. L. Beebe, V. S. Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process*, in Communications of the Association for Information Systems, 26(17), (2010) , 330

[266] B. Suh, I. Han, *The IS risk analysis based on a business model,* in Information & Management, 41, (2003), 150

[267] S. Alter, *a general, but readily adaptable model of information system risk,* in Communications of the Association for Information Systems, 14, (2004), 4

[268] N. L. Beebe, V. S. Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process*, in Communications of the Association for Information Systems, 26(17), (2010) , 330

software, and firewalls. The second is insider controls, such as policies and rules. The third countermeasure is detection and investigation capabilities. [269] We can generally see how there is already crossover between the criminology theories. Reducing opportunity through technical countermeasures and reducing motive through policies fit generally well within SCP and GDT territory. It is argued however, that a major problem of extending SCP theory within the cyber security realm is that it requires micro level analysis, and that appliance at the macro level analysis provides insufficient insight into the complexities of the offender environment where factors are manipulated to prevent crime. [270] The question thus remains, how can we truly measure and/or influence the behaviours accordingly and apply it in a relevant matter within IS security? While it is argued that it can be applied both to micro, meso, and macro levels, [271] we can also see that the appliance of SCP, or any criminology theory towards IS security for that matter, is already field tested and yields positive results. A relevant question should not be can we apply it, but analysing how we are successfully applying it and how can we improve it? Thus, with the contribution of criminology theories being rather unquestionable, are there more variables out there that can help organizations ensure ISSP compliance?

2.3.4 Multi perspective approach and categorization of ISP studies

It is implied that a multi-perspective approach for protecting an organisation's IS assets and resources is the best approach. [272] While many studies compliment ISSP theory with more or less the same criminology principles as this study, [273] other mentions of focus areas lie on other socio-organizational imperatives, [274] or technical aspects. [275] Generally, work on

[269] N. L. Beebe, V. S. Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process*, in Communications of the Association for Information Systems, 26(17), (2010) , 330

[270] N. L. Beebe, V. S. Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process*, in Communications of the Association for Information Systems, 26(17), (2010) , 330 – 331 ; R. Wortley, *Situational Crime Prevention and Prison Control: Lessons for Each Other,* in M. J. Smith, D. B. Cornish (eds.), *Theory for Practice in Situational Crime Prevention* (St. Louis 2003), 97 – 117

[271] [271] N. L. Beebe, V. S. Rao, *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process*, in Communications of the Association for Information Systems, 26(17), (2010) , 330 – 333

[272] P. Ifinedo, *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,* in Information & Management, 51, (2014), 69 ; T. Herath, H. R. Rao, *Encouraging information security behaviors: role of penalties, pressures and perceived effectiveness,* in Decision Support Systems, 47(2), (2009), 154 – 165

[273] P. Ifinedo, *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,* in Information & Management, 51, (2014), 70 ; N .S. Safa, R. V. Solms, S. Furnell, *Information security policy compliance model in organizations,* in Computers & Security, 56, (2016), 72 ; L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013), 449 ; T. Herath, H. R. Rao, *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,* in Decisions Support Systems, 47, (2009), 156 ; M. Siponen, M. A. Mahmood, S. Pahnila, *Employees' adherence to information security policies: An exploratory field study,* in Information & Management, 51, (2014), 219

[274] P. Ifinedo, *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,* in Information & Management, 51, (2014), 69 K. Rhodes, *Operations security awareness: the mind has no firewall,* in Computer Security Journal, 18(3), (2001), 27 – 36 ; A. Vance, M.

information security policy compliance can be categorized in three divisions: conceptual principles with no underlying theory or empirical evidence ; theoretical models with no empirical evidence ; and empirical work grounded in theory. [276] The first category presents guidelines and suggestions for improving employee compliance with IS policies. They aim to reduce problems. The second category provides theory based insights to how policy compliance can be enhanced, but lack any empirical evidence to support the insights. These models suggest social and technical solutions to reduce computer abuse and are often treated from the unique perspective and characteristics they offer as ISSP. [277] The third category presents theory based and empirically validated studies. Most of the studies done did not use integrated models (studies based on multiple theories), but rather single theories.[278] We can see this being changed however, in more recent studies. [279]

2.3.5 Current thesis contributions

Research on technical controls and policy compliance is abundant, but policy compliance and informal controls seem to be fairly rare, especially considering that respondents to organizational security effectiveness studies are usually not the end-user community. [280] It is important to understand that studies featuring formal controls also require social studies, as both formal and informal controls are featured in the GDT, but again this does not ensure true compliance being measured. That being said, it is noteworthy to mention that most popular theories in ISSP compliance feature some sort of theory related to criminology studies. I would like to emphasize again that within this thesis, the assumptions of grounded theory works with sufficient empirical evidence is further explored upon. Despite these works consisting of grounded theory, we can still see cyber incidents happening. Therefore, we delve deeper within the assumptions of the theory to discover how this is happening and what we can do about it. The financial and other ancillary costs involved with the increase in information security breaches clearly favour any attempt to improve the quality of prediction in order to reduce costs. [281] These costs are not only measured in monetary values, but also currencies such as a feeling of security, insecurity, and privacy for example. Cyber security encompasses so much more than technical measures these days, the human form and its

---

Siponen, S. Pahnila, *Motivating IS security compliance: insights from habit and protection motivation theory,* in Information & Management, 49(3), (2012), 190 – 198

[275] M. A. Sasse, S. Brostoff, D. Weirich, *Transforming the weakest link – a human/computer interaction approach to usable and effective security,* in BT Technology Journal, 19(3), (2004), 126 – 128 ; J. M. Stanton, K.R.

[276] M. Siponen, M. A. Mahmood, S. Pahnila, *Employees' adherence to information security policies: An exploratory field study,* in Information & Management, 51, (2014), 217 - 218

[277] M. Karjalainen, M. Siponen, *Towards a meta-theory for designing information systems security training approaches,* in Journal of the Association for Information Systems, 12(8), (2011), 526, 543

[278] M. Siponen, M. A. Mahmood, S. Pahnila, *Employees' adherence to information security policies: An exploratory field study,* in Information & Management, 51, (2014), 218

[279] L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013)

[280] T. Herath, H. R. Rao, *Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness,* in Decision Support Systems, 47(2), (2009), 155

[281] M. Siponen, S. Pahnila, M. A. Mahmood, *Compliance with information security policies: an empirical investigation,* in Computer (2010), 70

applications throughout the field intertwines in complex manners and deserves respective attention.

2.4. Summary of constructs

Compiling this vast amount of criminology theories in combination with IS security and insider threat literature might seem confusing at first. In order to more comprehensively grasp the subject, below is a table presenting the most important constructs and their referent descriptions per criminology theory, as well as the insider threat theory. Note that security compliance theory is not present, because I want to focus on using behavioural theory to reflect on contemporary cyber security practices in the field and ISSP is already baked in these theories.

Theory	Construct	Description
GDT	Deterrence	Refers to using mechanisms such as policies, guidelines and awareness programmes, to deter a certain behaviour.
	Prevention	Refers to mechanisms such as physical or procedural controls to deter a certain behaviour, should deterrence fail.
	Detection	Refers to mechanisms that address the realisation of computer abuse, aiming to make abuse known.
	Remedies	Refers to the treatment of consequences of a detected computer abuse, with action taken against the offender according to an organisation's policy.
	Formal controls	Refer to general deterrent strategies implemented by official controlling groups or individuals.
SBT	Attachment	Refers to a person's interest in the social surroundings, the level of acceptance of social norms and the development of a social consciousness with regards to his social environment.
	Commitment	Refers to the notion that people who invest time, energy, and effort in achieving social status, education, property or reputation are less likely to employ criminal acts that could jeopardize their achievements.
	Involvement	Refers to the idea that involvement in social activities leaves no room for engaging in criminal acts.
	Personal norms /	Refers to how individuals perceive their actions and the attitude they hold towards non – compliant

	beliefs	behaviour. Absence or weak beliefs in social values can fortify engagement in antisocial behaviour.
	Informal controls	Refer to social customs, traditions, norms, morality or other values implemented by unofficial controlling groups or individuals.
SLT	Differential association	Refers to the process where a person is exposed to normative definitions that either favour or appal criminal behaviour.
	Differential reinforcement / punishment	Refers to the idea of expected and/or realized reward and punishment resulting from criminal behaviour.
	Definition of behaviour	Refers to the attitudes about certain behaviour learned through the process of association, imitation and interaction or exposure to sources of learning in a certain social environment ; the moral attitude that defines an act as good or bad.
	Imitation	The engagement in behaviour after observing similar behaviour by others.
TPB	Attitude	Also known as behavioural beliefs, refer to the degree to which the person has a favourable or unfavourable evaluation of the behaviour in question.
	Subjective norms	Refer to perceived social pressures.
	Perceived behavioural control	Refers to the sense of self-efficacy, or ability to perform the behaviour of interest.
	Intention	Shaped through personal beliefs concerning the difficulty of realizing the related/intentional behaviour and the ability in successfully carrying it out. They are the immediate antecedents of behaviour.
	Facilitating conditions	Refer to conditions that either enable or hinder the performance of particular behaviour.
SCP	Increase the effort	Refers to increasing the difficulty of executing the criminal opportunity which may discourage criminal behaviour.
	Increase the risk	Refers to increasing the chances of criminal behaviour being detected and punished ; increasing the chances of

		'being caught'.
	Reduce the rewards	Refers to the reduction of the perceived benefit a criminal anticipates to receive.
	Reduce provocations	Refers to the reduction of precipitate or crime inducing situations.
	Remove excuses	Refers to the removing of the justification of criminal actions that appeal through moral judgements about offenders behaviour.
	Environment	Refers to the social environment surrounding a potential perpetrator of criminal behaviour as a means to facilitate opportunity.
	Accountability	Refers to taking or being responsible, liable or answerable for something that you have done or are supposed to do.
Insider threat	Insider	Refers to people within an organization that have the potential to cause damage
	Technology	Refers to technology based solutions towards human problems, such as auditing, layered access systems, access control, authentication etc. Can also refer to the systems or technology used by insiders
	Confidentiality	Refers to rules that limit access to information
	Integrity	Refers to the assurance that information is trustworthy and accurate
	Availability	Refers to the guarantee of reliable access to information by authorized people
	IS security	Refers to the entirety of securing integrity, confidentiality, and availability, both in itself and its elements, such as hardware, software, information, people, and processes.
	IS security policy	Refers to how organizations plan to realise their long term goals, described in terms of resources, processes and time path, in this case considering the (computer) and information systems.

	Malicious insider	Refers to the insider with a malicious intent to cause harm towards the organization in some way.
	Non – technical solutions	Refers to ways through which organizations approach the insider problem through non – technical terms, such as education, security training, and awareness programs.
	Non – malicious insider	Refers to insiders that carry a potential threat without having malicious intent. Incidents that they cause have no malicious intent and can be seen as accidental, often caused by careless, uninformed or negligent behaviour.

The goal of this thesis is wanting to investigate if these scientific theories are actually reflected in contemporary cyber security field practices. Traditionally, these constructs would be presented within a model, that is used to create a measurement upon which organizations can empirically test their current cyber defences. Instead of constructing a model and using quantitative analysis, I will be delving deeper into the assumptions that these models create and see how they hold up in practice through a qualitative analysis. Below in my methodology, I will explain how I will use these constructs and in a qualitative way measure their assumptions within the field and how I go about answering my research question by validating their empirical occurrence in the face of their theoretical preliminary assumptions in the literature review.

Chapter 3 Methodology

Through this extensive literature review, we have now gained insight in some of the general works within IS security and how technical and human factors attempt to keep the organizations safe. We have seen the many ways through which organizations can (try) to influence their users and to solidify policy in order to do so. By relying on the many theories, often grounded theoretical works, an abundance of models are available through which an improvement in security is attempted. Many of these models are translatable to a form of (enterprise) risk assessment, and by their quantitative nature present a visually appealing picture of where improvements can be made. In this chapter, I am going to explain my methods and the reasoning behind the choices I've made for these methods.

3.1 The quantitative nature of the field

How do we gain insight in cyber security in the field practices, and how do these measure up towards the current academic insights? As mentioned earlier, cyber security is dominated by a particular methodology. This consists of finding an analytical framework that deconstructs behaviour, adding constructs and/or groups that are not present in the model yet, either run a simulation based on existing data or create new data by sending out quantitative questionnaires, measure the new data, pull the measured data through a formula or program, accept or reject the hypothesis based on statistical significance, and finally conclude whether or not your new and improved model will lead to better security in the future.

While I will not argue that this is not the right way, I will argue that it is not the only way, and I will present the argument that this traditional approach of assessing cyber security problems has so far led us to cyber incidents still happening despite all of the improvements and added complexities towards various models meant to improve cyber defences. This method does provide us with statistical analyses. In fact, nearly all of the theories that I have featured in the literature review feature this kind of methodology.

3.1.1 Quantitative statistical analysis

So what do I exactly mean with this quantitative nature of the field I have been mentioning so often? In this chapter, I would like to present a small example of the quantitative statistical analysis that is usually performed within this field of cyber security in order to elaborate further on the pros, cons, and use these to be able to explain my choices in a better way. Different statistical methods are used in the models discussed in the literature review, each of them differing in some way, and each of them sharing some traits or resembling each other somehow. It is therefore difficult to elaborate fully on their methodologies, so I will shorty summarize them.

Most models feature a technique known as structural equation modelling (SEM). This includes sets of mathematical models, algorithms, and statistical methods that fit networks of analytical constructs to data. [282] SEM models are used to assess 'latent' constructs: (latent)

[282] D. W. Kaplan, *Structural Equation Modeling: Foundations and Extensions Advanced Quantitative Techniques in the Social Sciences* (2000), 79 – 88

variables that are not directly observed but inferred through a mathematical model using observed / observable variables. [283] A measurement model is used to define the latent variables while using one or more observed variables, and a structural model is used to impute, or attribute, relationships between latent variables. [284] Links between constructs of a SEM can be estimated using regression equations: statistical processes for estimating the relationship amongst variables. [285]

When exploring a SEM approach, it is important that a model is specified. There are two main components of models: the structural model, and the measurement model. [286] A structural model shows causal dependencies between endogenous (dependent variable in a causal model whose value is determined by the state of other variables) and exogenous (independent variable that affects a model without being affected by it) variables. The measurement model shows the relation between latent variables and their indicators. After a model is specified, the model has to be interpreted. This happens through path analysis, which is used to describe the dependencies between a set of variables. [287] After this, the "fit" of a model is examined. This is a determination through a 'goodness of fit' test, to see how well the model models the data: summarizing the discrepancy between observed and expected values, usually involving the examination of a random sample of unknown distribution to test the null hypothesis. [288] This is also the part where hypotheses are either accepted or rejected, based upon the statistical significance of the outcome of these tests.

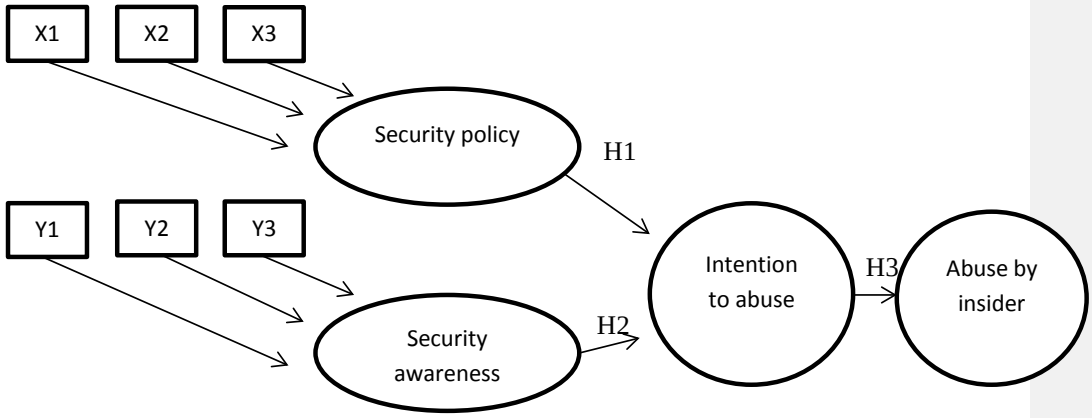
Validating these assessment models is done by looking at content, convergent, and discriminant validity. Content validity is offered through the representativeness and comprehensiveness of the variables used on a scale and examining the process by which these scale items are generated. Convergent validity, referring to reliability, is often done by using AVE: average variance value, which recommends the reliability of a measurement through a certain threshold. Discriminant validity refers to the correlation between measurements, ensuring that related and unrelated concepts remain separated. In the case of the models used in the literature review, this is done through looking at the square root of the AVE and determine inter – construct correlations by examining if items loaded more strongly towards their corresponding construct rather than other constructs.

3.1.2 Quantitative shortcomings

Drawing inspiration from multiple models used throughout the literature review, I have constructed a basic exemplary model below, featuring a basic SEM model with the attributed variables present in the table below. I have also formulated three exemplary basic hypotheses.

[283] B. G. Tabachnick, L. S. Fidell, *Using Multivariate Statistics* (Harlow 2013), Chapter 15 Multilevel Linear Modeling
[284] R. Kline, *Principles and Practice of Structural Equation Modeling* (2011), 230 – 294
[285] https://www.statisticshowto.datasciencecentral.com/what-is-a-regression-equation/
[286] K. A. Bollen, J. S. Long, *Tests for Structural Equation Models Introduction,* in Sociological Methods & Research, 21(2), (1992), 123 – 131
[287] P. Webley, S. Lea, *PSY6003 Advanced statistics: Multivariate analysis II: Manifest variables analysis* (Exeter 1997)
[288] H. M. Wang, *Comparison of the Goodness-of-Fit Test: the Pearson Chi-square and Kolmogorov-Smirnov Tests* (Taichung), 57 – 64 ; M. Olivares, C. G. Forero, *Goodness-of-Fit Testing* (Barcelona 2010), 190 – 196

To go with the model, as well as a hypothetical questionnaire to research the exemplary model. Please note that this is not an exact replica, merely a simplified version inspired from the original works in order to prove and visualize a point and explain why I refrained from this method, and adopted a qualitative analysis approach.



Concept	Construct	Construct variable	Measure description
General Deterrence Theory	Security policy	X1	Knowledge of security policy
		X2	Severity of security policy
		X3	Strictness of security policy
	Security awareness	Y1	Frequency of awareness programs
		Y2	Degree of security awareness
		Y3	Helpfulness of security awareness
Computer abuse	Intention to abuse	Z1	Intention to abuse ICT systems
	Abuse by insider	Z2	Frequency of actual computer abuse

Hypothesis 1	Security policy negatively affects intention to abuse
Hypothesis 2	Security awareness negatively affects intention to abuse
Hypothesis 3	Intention to abuse positively affects abuse by insider

Construct	Qnr.	Question	Answer
GDT			
Security policy	1	On a scale of 1 – 10, how knowledgeable are you on your companies security policy?	1 2 3 4 5 6 7 8 9 10 Not Extremely
	2	On a scale of 1 – 10, how severe do you feel your companies security policy is?	1 2 3 4 5 6 7 8 9 10 Not severe Extremely severe
	3	On a scale of 1 – 10, how strict do you feel your companies security policy is?	1 2 3 4 5 6 7 8 9 10 Not strict Extremely strict
Security awareness	4	How frequent does your company organize security awareness training?	……
	5	On a scale of 1 – 10, how much attention do you pay towards your surroundings considering security	1 2 3 4 5 6 7 8 9 10 No attention Too much attention
	6	On a scale of 1 – 10, how helpful do you feel a security awareness program is?	1 2 3 4 5 6 7 8 9 10 Not helpful Extremely helpful

A common denominator in these models, or rather a shared trait, is that new models add measurements by building on previous, empirically tested models. It should be noted however, that most of these models started gaining traction in the information system security field in the 1980s.

However, this method of building on and improving older models also carries limitations. General assumptions that have been made in the past do not necessarily translate directly into our modern society. With many variations existing among risk models, insider threat classifications, prediction models, and other cultural, behavioural models, a tradition of performing research has occurred, and with it, a tradition of standpoints that possibly limit our vision of how the concept has changed over time. [289] Background, history, culture, gender, language, education, all contribute towards a system of attitudes, beliefs, and ways of thinking. [290] I suggest we should forsake a positivist approach, but I do want to state that within this particular tradition of research we might oversee important aspects simply because the approach cannot cover them.

[289] H. G. Gadamer, *Truth and Method* (New York 1997), 302
[290] E. A. Herda, *Research Conversations and Narrative: A Critical Hermeneutic Orientation in Participatory Inquiry* (Westport 1999), 63

Let us consider an example. In a 2004 study, Lee, Lee, and Yoo present an integrative model of computer abuse, featuring SCT and GDT theory in order to provide a human factor oriented analysis to IS problems. [291] While concluding their findings however, contradictory to other studies, they find that deterrent factors such as willingness to install deterrence software actually leads to more insider abuse, and finding that the constructs of attachment and commitment were not significant to reduce insider abuse. [292] This is suprising, considering that these constructs are found to heavily influence deterring insider abuse in other studies. [293] How is this possible? The answer lies in the method of research, and the way data is acquired. Looking back at the exemplary quantitative research model, we can see for example that only three questions are formulated in order to measure the variable of security policy. Maybe there could have been more questions asked, perhaps there should have been better questions asked, perhaps the questions were misunderstood, perhaps some form of bias was present, such as giving politically correct or desirable answers. What if there were other (latent) variables that influence this construct, but have yet been discovered? This also occurs in the actual research done in the field and creates difficulty in conclusively assessing the subject. In other words, this quantitative research method does not seem to be able to probe deep enough.

Other factors that have to be accounted for, and who might skew the perception of variables, are that of outliers and insignificant data. Outliers occur, and statistical significance determines whether or not a variable is considered to be influential. In this process, and keeping the desired effect to be able to generalize the results, decisions occur to not include outliers or view data as insignificant. The positivist approach demands an emphasis on measuring variables and testing hypotheses, what counts as significant is decided beforehand. [294]

These described problems arise due to a limited ability to probe for answers. Data outliers within SEM methods are often discarded or excluded from analysis. From both a security mind and academic perspective however, this is unwanted. [295] A common statement in the field is that 99% security means 100% vulnerability. [296] This is due to the fact that no

[291] S. M. Lee, S. G. Lee, S. Yoo, *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004)
[292] S. M. Lee, S. G. Lee, S. Yoo, *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004), 715 – 716
[293] Q. Zhai, M. Lindorff, B. Cooper, *Workplace guanxi: its dispositional antecedents and mediating role in the affectivity – job satisfaction relationship*, in Journal of Business Ethics, 117(3), (2013), 550 ; L. Cheng, Y. Li, W. Li, E. Holm, Q. Zhai, *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013), 455 ; P. Ifinedo, *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,* in Information & Management, 51, (2014), 75
[294] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches* (Essex 2014), 167
[295] https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html ; https://www.theanalysisfactor.com/outliers-to-drop-or-not-to-drop/
[296] https://www.cerias.purdue.edu/site/blog/post/featured_commentary_the_honorable_mark_weatherford_dhs_deputy_under_secreta/

workable system is 100% secure, [297] as this requires the system to be completely stagnant. In the field, security vulnerabilities are not static: they evolve, are a continuation or iteration of previous vulnerabilities, or new vulnerabilities arise. These vulnerabilities appear as outliers: previously unknown (or willingly ignored) low occurrence incidents. That one outlier, the less than 1%, could be the difference between safety and an actual data breach. To view something as insignificant without knowing the full consequences is a dangerous assumption within the field. But what does this mean from an academic perspective? Here, these outliers are important as they present new variables. Just as in the field, outliers have their place within analysis. Their low occurrence does not easily lend towards generalization, but seeing as that within this thesis we are looking to what extend academic insights match in the field practices, and we are exploring a field where outliers are a core aspect, I want analyse differently which other methods allow me to do. Outliers could thus be measurement or recording errors, or unintended outcome of set definition. But, they can contain valuable information, rather than appear meaningless aberrations caused by errors. Hence, it is important to ask what their meaning could be and what they can teach us.

3.2 Holistic approach and qualitative research

It has been mentioned earlier in the literature review, that a holistic approach towards cyber security problems is a must. In the previous section, we have determined that a quantitative approach alone is not enough. The data does not tell a full story, and to assess how academic insights truly occur in the field and are applied, we require other methods. In research, triangulation of methods ensures a holistic approach. [298] The generalized frameworks produced in quantitative analysis are experimental in their nature: the results are expected to be the same if the experiment is repeated in the same environment. Human behaviour however, is much more complex than this and does not easily lend itself to quantitative measurements. The insider threat is based on bias, ambiguity, and is behavioural in nature. Context is never truly the same. Qualitative analysis however is known for its use in social and behavioural studies. The ability to probe deep and obtain rich and descriptive data allows for a structured way to immerse within the subject and provide solid grounded theory. [299]

3.2.1 The merits of qualitative research

Qualitative research methods can be used to gain further insight. Qualitative research is known for the ability to perform case studies. Case studies can be seen as an experiment to test if a certain theory occurs, or as an instance or illustration of a principle. It is a detailed

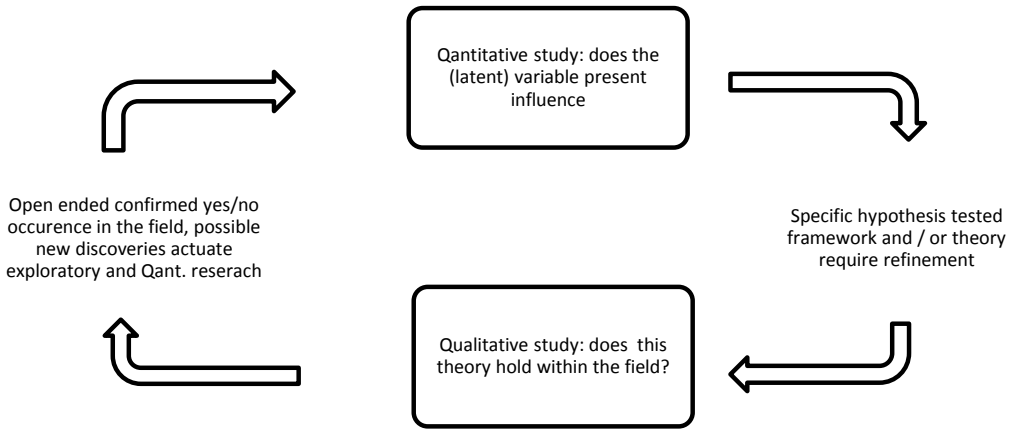
[297] https://www.quora.com/Is-it-ever-possible-to-prove-a-system-is-100-secure ; http://bhconsulting.ie/remember-there-is-no-such-thing-as-100-security/ ; https://www.compuquip.com/blog/top-5-cybersecurity-threats-and-vulnerabilities ; https://www.solarwindsmsp.com/blog/it-possible-never-experience-it-security-breach ; https://www.techrepublic.com/article/100-of-corporate-networks-highly-vulnerable-to-attacks-heres-how-to-secure-yours/

[298] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches* (Essex 2014), 166

[299] P. G. Swanborn, *Case Study Research What, Why and How?* (London 2010), 18

examination of a subject of study, which also could lead generalizable theoretical propositions, and can aim to create and expand rich these theoretical frameworks. [300] Validity occurs through assessing what is claimed to be researched, the appropriateness of the tools, processes, and data used. Qualitative research seeks answers for questions of "how, where, when, who, and why". [301] The goal is to add enrichment to subjects after quantitative analysis, or if these cannot be (easily) quantified at all. Truthfulness and achieving authenticity (this means validity in qualitative research) comes from creating a tight fit between understandings, ideas, and statements about the social world we are trying to explain and what is actually occurring in it. [302] Reliability for qualitative research lies with consistency of the processes used and transparency regarding the choices made.[303] This can be done through various techniques, including solid determination of how you conduct your interviews and how you handle your observations.

It is important to not become locked into a positivist idea of replication, equivalence, and subpopulation reliability, but to accept the idea of data collection as an active, interactive process, where the setting and context evolve and can illuminate different facets or dimensions of a subject matter. [304] The goal is to reach where research has not gone before, to form and refine coherent theory and make sense through organizing data and comparing them to the preliminary ideas about the subject matter. This is why I choose to apply a qualitative research model within this thesis, to get to the bottom of the problem, to take on a perspective of how scientific cyber security discoveries hold up in the field. This might contribute to how IS can be improved in the future, with a focus on the human factor and insider threat. Below, I present an illustration of the importance of the qualitative methods and how I aim to use them in this thesis.



[300] P. G. Swanborn, *Case Study Research What, Why and How?* (London 2010), 66
[301] L. Leung, *Validity, reliability, and generalizability in qualitative research,* in Journal of Family Medicine and Primary Care, 4(3), (2015)
[302] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches* (Essex 2014), 218
[303] L. Leung, *Validity, reliability, and generalizability in qualitative research,* in Journal of Family Medicine and Primary Care, 4(3), (2015)
[304] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches* (Essex 2014), 218

3.2.2 Examining policies

We have seen that both quantitative and qualitative practices have their own merits, so how do I go about applying qualitative methods to measure what I want to know? In my literature review, I have used the same criminology theories as Theoharidou et al. [305] In their study, they identify what is currently missing from IS policies, set up a framework that applies insider threat and behavioural theories derived from criminology, and then measure in existing policies (ISO17799 in particular) whether or not the policies have incorporated these behavioural assumptions. This is done by scanning for words containing the subjects of the behavioural theories from criminology. The chances of those exact words occurring is fairly low however, but that does not rule out that they were not thought of during the policy formulation process. Scanning for the occurrence of words does not necessarily reflect the way through which the policy was constructed and with what values or theory in mind. Since most policies are not static, [306] the analysis of a finished product stands in the way of a more holistic view on reflecting whether or not scientific insights are applied in the field. A second problem arises when looking at policies such as ISO 17799:2005 (or its current version: ISO 27002:2013) because it is an international standard code of practice for information security management that offers guidelines and general principles for information security. [307] This means that it does not always suit the needs for a variety of businesses and organizations of different natures, and therefore does not allow us to delve deep enough in how academic insights occur in the field. Considering these ISO standards are not bound by law, I suspect that many organizations either do not have these applied, or that their organization has to deviate from them anyway, opening up more possibilities with regard to the main research question as to how insights are applied in the field.

3.2.3 Performing qualitative interviews

Merely scanning for words occurring in policies is therefore not reliable enough to probe deeply. And how do I exactly determine which policies to inquire? Are organizations willing to share their policies? Do they like to talk about (potential) security hazards and their own vulnerabilities? And even if I get to explore an organizations cyber security policy, I do not get to see the problems that end users might have, or what other levels of an organization face, I only get to see what the policy writer believes the end users are facing and what the policy writers intentions are. To overcome these issues, I employ open ended questionnaires, used during interviews, to find out whether the scientific insights in the cyber security area are actually applied in the field. I choose interviews because this enables both me and the interviewee to explain and clarify questions and answers if they are misunderstood or require more elucidation. The personal connection established during a face-to-face interview gives the opportunity to elaborate when misunderstandings occur and helps respondents to share information in their own words and experiences and make sure that people who can talk about

[305] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security 24, (2005)
[306] V. Tangcharoensathien, P. Jongudomsuk, *From Policy to Implementation: Historical Events During 2001 – 2004 of universal coverage in Thailand* (Nonthaburi 2004), 3 – 107
[307] https://www.iso.org/standard/54533.html

this subject don't withhold their answers due to not recognizing a certain construct while actually being familiar with it, or seeing ways in which the constructs are applicable or applied within the field.

But who should I interview and why? What is a correct sample size and who would recognize the behavioural theories used in this thesis? During the formulation of this thesis, whilst gathering more background information about IS security in general, I approached various IT / ICT administrators, who have requested to remain anonymous, asking about their cyber security policies and the thought put behind it. I noticed that a lot of these people tended to have a very technical background, with little to no knowledge of the social sciences and their applications within the cyber security field, and relatively poor oversight in the ways end user policies were constructed apart from the technical perspectives, such as for example general deterrent factors such as a firewall, two factor authentication, etc. It would appear then, that questions about behavioural theories could not be answered to their full extent, while I suspected these would actually occur often in the field. Therefore I decided to not contact organizations themselves, but a more neutral party assisting these organizations with their cyber security defence: some of the Netherland's leading organizations in cyber security advisory. These organizations, such as KPN Cyber Security, but most of whom I cannot name due to agreeing for them to remain completely anonymous, provide advise towards organizations on best practices for their cyber security.

The reason I sought to interview cyber security consultants is because they have insight in a lot of organizations, their policies, cyber defences, and probable shortcomings. Therefore, it is likely that these consultants have relevant knowledge about the subject matter and in the field practices. With the promise of remaining anonymous, I reckon to be able to get a lot of relevant data that I could not get if I approached their customers (organizations with cyber problems) myself. Their expertise as well as their experience in the field, combined with their constant strive to keep up to date with cyber security gave me the highest likelihood of understanding whether academic insights are applied in the cyber security field or not.

In total, five interviews will be used to answer the research question, with the participants being: a strategic advisor of information security ; a manager of business, security, security services, research and development ; a forensic senior manager, a senior manager cyber IT advisory with a technical background, a senior consultant cyber IT advisory with a non-technical background. These participants were asked to conduct a forty five – sixty minute long open question interview, regarding cyber security policy, the human factor, and insider threat. As mentioned earlier, these organizations are leading in cyber security advisory. This is why the sample size is relatively low, but relevant.

3.2.4 The questionnaire

Constructing a questionnaire to get in depth answers requires some nuance. Having closed questions results in possible closed answers while the might be some interesting information lurking. Having a too long interview might tire out and annoy interviewees, while having a too short interview might not give us enough information to deal with. Below, I will present my questionnaire, translated from Dutch to English. It encompasses the constructs gathered in

the literature review and intends to find out in the field practices and overlapping themes with academic literature. At first glance, the questions might seem ill-defined due to a lack of consistent affirmation that we are talking about cyber security for example and not regular security. It should be noted then, that all of these persons already know that we are talking about their expertise area, which is cyber advisory, and that repeatedly using the same specifics within questions tires people out, irritates them, or gets them bored and distracted. The questions are designed to trigger responses and don't narrow down too specific in order to get the interviewees to talk more openly about the subject matter. The open ended nature of qualitative questions is kept in mind here.

Insider threat
According to the theory and when we look at the biggest (and most costly) incidents, the danger of the own employees of a company who can cause the most damage is bigger than external threats.

Q: When we look at threats that can possibly cause a lot of damage, are internal or external threats the most important focus area according to you and why?

Q: Considering internal threats, how do you see the proportions between accidental and malicious incidents and how does policy formulation account for this?

Q: How do you see the connection between a workable work environment and a safe work environment?

GDT (General Deterrence Theory)
According to the theory, criminal behaviour can logically be explained through maximization of benefits and minimization of downsides. Insiders within an organization could act from this principle and strike when they find that an action could reap them lots of benefits.
Catchwords:

- Deterrence
- Prevention
- Detection
- Remedy
- Formal controls

Q: Looking at maximization of benefits and the minimization of downsides for potential cybercrime, what do you believe, on a general level, should be accounted for?

Q: Policy often grows from specific occurrences. What is, according to you, an effective division of attention considering general and specific cyber defence?

Q: Do you advice cyber policy on the basis of a certain standard or do you prefer to apply 'custom made' tactics?

SBT (Social Bond Theory)
The theory states that weak social connections / bonds can motivate criminal behaviour. The insider within an organization could decide to strike due to little affinity with the organization or a lack of loyalty.

Catchwords:

- Attachment
- Commitment
- Involvement
- Personal norms / beliefs
- Informal / social control

Q: Do you believe that employees have a natural tendency towards criminal behaviour that has to somehow be supressed?

Q: Do you see possible application for informal control (e.g. social bonds, social control) within cyber security policies?

Q: How do you see the possibility towards influencing the attitude of employees against non – conform security behaviour?

SLT (Social Learning Theory)
According to this theory, criminal behaviour is learned or copied. The insider could be influenced by behaviour he copies from others, or behaviour that is expected of him by his colleagues, but is not conform the security policy.
Catchwords:

- Learning behaviour
- Copying of behaviour
- Imitation of behaviour
- Moral attitude towards behaviour
- Social environment

Q: During the formation of policy, is the eventuality of learning, copying and imitating 'bad' (read insecure) behaviour kept in mind?

Q: What is, according to you, the influence of a company's culture on its employees and how important do you deem this role?

TPB (Theory of Planned Behaviour)
This theory states that intention precedes behaviour that inclines towards abuse or non – conform behaviour and therefore plays a pivotal part in the explanation of behaviour. Attitude and personal thoughts about certain behaviour can both motivate and deescalate certain behaviour.
Catchwords:

- Attitude
- Norms
- Intention
- Facilitating conditions

Q: Is there a current role within security policy to influence the intention towards non – conform behaviour to prevent cyber incidents and how is this done?

Q: What does the role between intention and actual execution of behaviour look like when considering accidental and malicious incidents?

SCP (Theory of Situational Crime Prevention)
According to this theory, criminality does not only occur when there is motive, but also when there is opportunity. An insider that at first hand has no plans to perform a certain action, could be convinced to actually follow through once he realises an opportunity exists.
Catchwords:

- Effort
- Risk
- Reward
- Provocation
- Excuses
- Environmental factors
- Responsibility
- Accountability

Q: Will conditions that could potentially provoke or hinder non conform security behaviour be taken into account within cyber policy?

Q: Do the factors, 'effort, risk, reward, provocation, and excuses' have a current role within a security policy?

Q: How are the factors of accountability and responsibility being dealt with in a cyber policy?

Final Question

Q: In your opinion, where is the biggest area of potential growth in the field of cyber security? In what area and in what way?

3.2.5 Limitations of this methodology

The use of this qualitative methodology also limitations of as well. Qualitative research lends itself to deep probing, but it is harder to generalize. This hampers its usability in a standardized model that can be applied in the cyber field. I have mentioned earlier how ignoring outliers can pose a security problem, and how the same cyber security model could not always be applied towards different organizations: the same is true for a qualitative approach: not every organization deals with the same outliers and problems.

Another limitation of this study is the relatively low sample size. Though the organizations involved are currently leading in the field, a higher sample size might increase the validity of the study. Another aspect to keep in mind is that through these interviewees, only organizations actively seeking cyber advisory or organizations who were approached by these cyber advisors are considered. Though an argument could be made that in general organizations featured through these interviewees are a reflection of all organizations within the Netherlands, especially considering that one of the firms represented in the interviews hands out relatively affordable advice. I mentioned earlier how outliers are an important

aspect within this thesis, through only conducting interviews with cyber advisory firms, it is possible that I miss important outliers currently unknown to these firms that could prove to be interesting topics within this thesis.

A third limitation of this study is the lack of an observant or anthropological study. Observation of the work floor could improve and contribute to the relationship between the preliminary theory and acquired data. Conducting interviews with actual end users, management, and organizational levels would grant me a clearer picture of what happens at those divisions. In the future, I would therefore recommend that the results and conclusion of this study would be used in a new quantitative analysis in order to analyse how effective change made around the suggested constructs in this thesis would be. The next step would be to observe how these changes play out at the different levels inside an organization, and together this will enable to tell us how successful the improvements actually are. As mentioned before, qualitative science fills the gaps where quantitative science cannot reach. They should not be viewed as opposite, but accepted for both their merits and their flaws and be seen as complementary instead of contradictory.

Chapter 4: Results and analysis

Below, I will present the results of the interviews, summarized per question, and analysed in regard to their preliminary theoretical scope per theory. Each chapter will therefore feature a theoretical preliminary assumption, where I summarize the subject as treated within the literature review. This will be followed by a summary of the questions per subject and the answers given by the interviewees. Each chapter will be closed off with an analysis, where the assumptions made by the theory and the empirical results will be mirrored and in this way the academic literature will be tested with in the field occurrences. Note that these interviews have been anonymized, and can therefore not be used to track individual responses towards a certain organization, person, or the methods, techniques, processes and procedures of that organization. For readability, I will refer to the interview with the senior consultant cyber team IT advisory (non-technical background) as "Person 1"(P1), the senior manager cyber IT advisory (technical background) as "Person 2" (P2), the business, security, security services, research and development manager as "Person 3" (P3), the forensic senior manager as "Person 4", (P4), and the strategic advisor information security as "Person 5" (P5). The original transcription of the interviews can be found in the attachment. These have not been translated towards English to preserve their integrity.

4.1 Insider threat: theoretical preliminary assumptions

The insider has the potential to cause more damage than an outside attacker. The threat originates from people who are given access to an information system, but misuse their privileges and violate IS security and ISS policy, either accidentally, or intentionally. The involvement of multiple parties within the business opens up a plethora of new risks. The insider threat can be examined in the context of changing technical, social, business, and cultural factors. Currently, methods exist that combine both technical, organizational, and behavioural models to assess and hopefully reduce the insider threat. An holistic approach that combines technical, behavioural and organizational factors is rare, but efforts are being made. Education, security training and awareness are generally seen as some of the greatest non – technical measures available, in order to promote security compliance intention. An exploration of these factors can be done in the context of intention, separating malicious intent from accidental occurrence. Through this path, poor usability of a system can severely hamper its security. The insider threat can be viewed in a broad perspective of technological, organizational and behavioural factors, that seek to influence him.

4.1.1 Internal versus external threat

The respondents were asked to answer the question: 'When we look at threats that can possibly cause a lot of damage, are internal or external threats the most important focus area according to you and why?' According to P1, it appears correct to state that the insider threat is increasing, but it is not correct to state that it is the biggest threat. External threats carry a bigger risk potential, especially when considering that even for example nation states are a big player in cybercrime. More focus on the insider threat is good however, and required especially considering third and fourth parties being heavily involved in modern businesses.

P2 states that the perception from most of their customers is that external threats are the largest, and a great portion of the measures, including policy, is aimed towards countering this outside threat. Meanwhile, a great portion where P2's own organization spends their attention at, is underlying culture drivers that an organization needs to make internal threats visible and prevent them from being misread.

P3 states that when looking at the possibilities, the internal threat is the most important, but when you look at what occurs in the field, external threats are mostly regarded at the most important area. When looking at reports, we can conclude that the biggest risk comes from the insider, accidental or malicious, with a potential of great damage. The actual most damage however appears to come from the external malicious side.

P4 brings up that both are equally worth to be considered. Internally, the most important considerations should be made where the most important assets are exposed to risk. There is an important distinguishment between accidentality and maliciousness, and there is certainly a connection between external motivators for internal incidents. It is quite possible that external threats target insiders because of shared interests or because they understand insiders accidentally screw up, facilitating the external threat.

P5 explains that depending on the scope, external threats are usually focussed upon. This depends on the domain and sector however and how this domain or sector decides whether or not you are actively trying to stay ahead of external threats. The development of human factors as threats and the way through which accidents are taken into account contribute toward this, even though you should not look at the measurements that you take, but the effect that you are trying to accomplish. As of now, vulnerabilities are actively searched upon, primary causes and risks are identified, and actively regarding the effect that you are trying to prevent sometimes gets lost in this process.

4.1.2 Accidental versus malicious incidents

In order to understand the relationship between accidental and malicious insiders, respondents were asked to answer the question: "considering internal threats, how do you see the proportions between accidental and malicious incidents and how does policy formulation account for this?" P1 answered that there is a difficulty with actually measuring the impact of malicious insider threat, as companies don't want this kind of information to go public, and would rather pose the incident as accidental. Therefore, it is difficult to truly assess the impact of data leaks caused by malicious actions. Even with the General Data Protection Regulation (GDPR) and thus the Dutch AVG (General Regulation of Data) there is a duty to report incidents, but not their nature. In policy people tend to account for the difference, explaining how data should be managed and what happens when handling data goes wrong. This is also a judicial question: who is accountable? Many different insights regard this topic and there is a big grey area patched through codes of conduct, codes of ethics, and norms of behaviour.

P2 states that our goal here is mainly to prevent, detect, and respond. In practice, both accidental and malicious incidents occur. Safety nets are in place to mitigate unintentional

mistakes and there are several detection measures to keep an eye out for people who are acting out of the ordinary.

P3 answers that when we are looking at the insider threat, we are talking about employees, suppliers, business partners, third parties, etc. It is healthy to make a separation between who is able to access certain internal facilities. If we look at malicious insiders, every organization has a 'rotten apple' or two. Those who seek to do no good will consciously seek the borders, while accidental incidents should be viewed as non-intentional. Certain policies are in position to ensure that malicious insiders don't gain access to the organization at all, such as screening during job applications and regular background checks. Regular assessments are in place to ensure that accidental incidents through careless work are prevented. Eventually, these matters of integrity are also broader than cyber security alone, it is about permissible and impermissible behaviour.

P4 indicates that culture and behaviour within organizations are important. Our behaviour is very dependent on our environment. Creating an environment where people deem it important to handle confidential data well and where clear, good rules exist and procedures are constructed to help assist people to do good business, is inherently less prone to incidents than organizations where there is no attention for such things. Places where management does not emphasize on the importance of information security, where employees don't dare to open up on mistakes or admit wrongdoings or incidents, those places are more prone to incidents happening. Within an organization, about 5% of the employees are exquisite. There is also about 5% of the employees who will always screw up in any way possible, either incidental or not. The important focus area is the remaining 90%, that has to be influenced through a healthy culture and environment that the behaviour of the first 5% is wish able, leaving the chances of malicious threats to decrease. P5 explains that malicious and accidental incidents are seen as two separate sources, and that there is a lot of difference in how separate companies deal with this. Organizations that are affiliated with the safety field tend to focus more on the accidental incidents because they assume there is a safety situation where people don't intentionally screw up.

P5 believes that now, contrary to a few years ago, more attention is given to people that might potentially harm your organization from within. When constructing policy, human factors tend to be taken more seriously nowadays. There is a difference between awareness, and actual identification form potential negative behaviour that could damage the organization.

4.1.3 Work environment and safety

Keeping the facet of poor usability in mind, I asked the respondents to answer the question: "How do you see the connection between a workable work environment and a safe work environment?" P1 answered that the culture that you have within an organization has to be configured to how security, which is often seen as awkward, clumsy, extra work, annoying, or not relevant, is being seen. Typical tension fields arise, people just want to do their jobs but they suddenly have to do all sorts of extra work. The culture that you have within an organization has to be configured to how security, which is often seen as awkward, clumsy,

extra work, annoying, or not relevant, is being seen. Typical tension fields arise, people just want to do their jobs but they suddenly have to do all sorts of extra work. The culture that you create can influence this in a positive way. If there is room to approach your colleagues, but also your superiors and vice versa, you create a safety culture that keeps everyone on board and makes them extremely conscious and aware. This shows that there is room for a congregate of workable and safe.

P2 also notes that this is always a tension field. This is always a tension field. The security realm, for example a CISO (Chief Information Security Officer) wants to up security to way beyond the acceptable or even allowed norms of the business field. Depending on the governance within an organization, certain measures might be or not be implemented. It is very hard to configure this in a way where the business field is not obstructed in some way by the security field.

P3 recognizes that security versus usability is a recurring battle. Security versus usability. Those within the security realm seem to think in ways that elude the average person's mind. A safe work environment is essential to keep the work environment workable. End users don't want to experience any nuisance though from the security perspective though. It is most important that we look at what the core feature of an organization is, and that the security field enables them in doing so. End users don't want to be bothered with difficult and complex safety precautionary actions, they want to do what they want to do, for example, a doctor wants to make people healthy and not think about whether his patient files are stored secure enough. Most people are not preoccupied with security, they only care for a workable work environment. It just happens to be, that this work environment has to be facilitated by a secure environment. Therefore security is important, but people must not experience burden by it, or at least understand why it is in place.

P4 supplements that scientific research has been done within the medical world concerning this topic. Sections of the hospital that featured no rules averaged around 12 incidents per time frame. Sections that featured a few rules, averaged around 9 incidents per time frame, a positive gain. It appeared however that sections that had very many rules, averaged around 23 incidents per time frame. Too many rules prevents people from thinking for themselves, disabling the process of making connections and seeing why things are. Secondly, people who are imposed with more or even too many rules become nervous because they are afraid to violate any of those rules: hypegiaphobia, eventually resulting in the actual violation of those rules. Thirdly, imposing too many rules creates aversion and an incline to deliberately violate the rules. As far as a workable work environment is concerned, this has to be facilitated in terms of time for execution, resources, means and knowledge to develop competence to do what you want them to do. Putting people under pressure leads them towards focusing only on the things they perceive they can still do, they will then always take the shortest route and forget or not even see problems that lie in their wake. Therefore there must always be a healthy balance between rules and trust: a certain sweet spot.

P5 sees this as a net process. There is a difference between being able to safely perform your work, or to work safely. The former puts the users in the primary process in a central

position, the latter tends to lean on a security perspective that features the necessity of performing certain measures. What we should want, is an environment that looks at what you must do and how this can be facilitated through the most safe way. Safety has become a 'container term': what is safe for one, is problematic for the other. Security and business are factually seen as opposites, as if they are contrarian, and that is one of the biggest issues with security at this moment. Security thinks they are supporting the business, but factually they are not. Inside an environment where the context or setting of a process changes, certain measures can be either helpful or impairing. In our current society, we must be able to perform dynamic work with changing infrastructures. A stark regime of measures and rules, paired with the many activities one must perform in conjunction with his regular work leaves us with an unsure relationship between security and business. Too many measures are being thought of, because someone some time ago worried himself, but those worries come from a security perspective, and the end user is stuck with entirely different problems. A working situation occurs when you have security people that talk the talk of business. You can question how central the end user is when you have to explain him how to do his job, contrary to when you help him do his job.

4.1.4 Insider threat analysis

The empirical evidence suggests that the insider risk is increasing, and its potential to cause unrecoverable damage is there. However, it does not necessarily become the biggest threat. There is a difference between what is possible, and what happens in the field. Perception on where the biggest risk lies is divided, depending on the scope, domain, and sector. The involvement of multiple parties within the business area, including third parties, nation states, and others, brings about new risks as more and more gain access to an information system, and can possibly abuse their privileges herein. Though the interviews indicate that most focus is aimed towards the external threat, all interviewees indicate that the insider threat is either equally or more important than the external threats. It is interesting to notice how P4 also mentions that external threat agents can somehow seek to target insiders due to shared interests, or through using them to facilitate this external threat. This blurring of the boundaries between insider and outsider is also exemplified in chapter 4.6.2 where P5 explains it is difficult to assess the separation between an insider and an outsider, considering how certain 'hacks' are often the result of retained credentials opening up opportunity for criminal behaviour.

There is thus a difficulty in truly grasping the impact of malicious versus accidental insider incidents. According to the interviews, we know both occur in the field, but organizations are reluctant to share cases. Safety nets, such as policies, assessments, and procedures, are often in place to mitigate unintentional mistakes and there are several detection measures to keep an eye out for fraud. Despite these, incidents still happen. Third parties that gain access to systems bear a high risk with them, as well as 'pure' insiders, as every organization has a small percentage of 'rotten apples' that will always pose a risk despite the best efforts. It is according to the interviews important that management emphasizes on the importance of information security, to keep the majority of its employees in a healthy security environment. On an interesting note, despite the implementation of the GDPR, the actual nature of a data

breach is often still shrouded or at least not made public. When looking at the proportions between accidental and malicious incidents, we can see that organizations have a main goal of prevention, detection, and response, with safety nets in place to mitigate unintentional mistakes and response and detection should things still go awry. These safety nets have accidental and maliciousness in mind. Regular assessments could for example be put in place to ensure that accidental incidents through carelessness is prevented, and certain policies exist to ensure that malicious insiders' don't gain access to the organization at whole. The interviews indicate that over the years, more attention has come towards the insider incidents and the human factor in general is being taken more seriously nowadays. This does not mean however, that these incidents are far from over.

One of the most important contributors, according to the literature review is human behaviour, and the interviews already concur this within the first topic. Culture and behaviour within organizations is important and behaviour is dependent on our environment. This environment can be influenced to attract wish able behaviour, but there are two sides towards this coin as a culture of fear or otherwise 'diseased' culture can actually promote criminal behaviour. This topic will be treated more in depth during the behavioural topics within this results chapter. As for now, the interviews indicate that culture within an organization has to be configured to make security, which is often seen as awkward, clumsy, extra work, irrelevant, or annoying, part of a broad sate of consciousness and awareness. Tension fields arise, as the security realm often clashes with the business field. Security versus usability should however not be seen as contrarian, but as supplemental, a net process. It is essential that security facilitates workability and does not burden it. It is hard, but not impossible to configure this. Too few rules lead to incidents, but too many rules lead to more pressure, more incidents, hypegiaphobia, or even an aversion for the safety culture in general. What is safe for one, is problematic for the other, the two sides of business and security focus too much on their own perspective, they do not speak the same language, and this is becoming a problem.

As explained by the interviews, security versus usability is a common issue in the field. With more safety nets having to be applied within organizations to counter the rising internal and external threats, the work environment of end users could potentially be harmed in a negative way. We have seen how too many rules can lead to unsecure situations in the interviews. According to these interviews, tension fields typically arise as people just want to do their jobs, but security steps in with their own problems. It would appear that a corporate culture that enables a safety culture and keeps everyone aboard, conscious, and aware, is a solid way to handle this problem. This is in line with the insights of the literature review, that states how security training and awareness are seen as some of the greatest non – technical measures available to promote security compliance intention. With a tension field existing between the security realm and the business side, the interviews indicate that it is important that end users are not too hindered in their work, while a safe workspace is still facilitated as this is important for security as well. In the end, it is about finding a sweet spot that works for a specific organization, and keeping up to date with security trends to ensure the security does not become a burden, and actually facilitates the business.

4.2 General Deterrence Theory: theoretical preliminary assumptions

In its core, GDT assumes logical decision making at the maximization of benefit in combination with the minimization of cost. Expected outweigh of benefit against the perceiving cost might motivate an insider to strike. Through this reasoning, it expects to tackle computer abuse before it actually happens by removing the motivation for it, or through minimizing the (expected) benefit. The most important aspect of GDT is knowing that anticipating motive and adjusting behaviour accordingly through the means of deterrent techniques will have a positive result on declining computer abuse. Some examples of these deterrent techniques constitute of technical means, such as anti-virus software, but also organizational, such as having an information security policy, or through processes, such as through applying a security action cycle. An action cycle often includes stages of deterrence, prevention, detection, and remedies. These stages all have their formal and informal controls, including policies, guidelines, and soft – and – hardware. As its name suggest, general deterrence remains on a general level, being an applicable concept throughout various organizations, and consists of implementing (basic) security controls to create a deterrent situation.

4.2.1 Balancing benefits and downsides for potential cybercrime on a general level

With the core concept of GDT being the maximization of benefits and the minimization of downsides for potential cybercrime, respondents were asked to answer the question: “Looking at maximization of benefits and the minimization of downsides for potential cybercrime, what do you believe, on a general level, should be accounted for?”. P1 answered that it starts with prevention, ensuring authorization control is in place, and restricting access to the databases, as well as physical access requiring a strict infrastructure. Detection, monitoring, and respond follow suit. There are two sides to this topic. At first, good technique and proper tooling that detects what you want, that can pick up on detection and offer you handles to plot action. The second side is process: ensuring that everyone knows what they must do. Crisis management is in order: knowing who to communicate to when things go awry and knowing where responsibilities lie. Fact checking is a must, and acting on assumptions is out of the question.

P2 supplements that there is a combination of authorization, detection, and response. In general, also considering insider threat or fraud, you can try to always be one step ahead, but cyber incidents are going to happen anyway. Gaining access is not the point, the main point is remaining hidden. This is where we can gain the most profit in our field: detection. Prevention is a must, but it is an illusion to assume incidents will not occur. Detection must be swift in order to mitigate and control the damage.

According to P3, one of the major grounds of criminal behaviour is opportunity. A system such as the ‘4 eye principle’, which separates functions and responsibilities, works because opportunity is reduced. The same person that checks incoming factures for example does not check the payments of those. Besides that, Cyber Security Build Nederland describes how important basic controls are. In the experience of P3, lots of organizations lack basic controls, like anti-virus, firewall, a security policy, the basics really. Lots of parties don’t take basic security measures, they don’t implement them, they lack the controls, and things go wrong. It often requires an incident at first to gain traction for action.

P4 shares the insight that everyone sees different benefits, with the most obvious ones being money, status, and interpersonal relationships. One of the most important downsides is being detected during illegal activities. One could benefit from figuring out how to give the suggestion that what people are doing will be noticed and seen, which is a matter of supervision. It is scientifically proven in multiple ways that supervision works, but sometimes it is also essential that it is shown where the border of acceptable behaviour is, and have one example cross that border to exemplify to the rest what is unacceptable. Supervision in a discernible way is true general deterrence.

P5 notes that primarily, on a general area, you can ask yourself what the negative effects are and then see if these are detectable or not. What happens now, is that a lot of measures are thought – and – made up that are supposed to prevent a negative effect, and the performance of these measures is being scrutinized for effectiveness , but gauging if the measure is effective in countering the negative effect that you wanted to prevent in the first place, is sometimes lost in the process. All effort is put in coming up and auditing of the measures that must be executed, instead of focusing on what your actual primary goal was in the first place. P5 notices that this occurs often in the field.

4.2.2 Division of general and specific cyber defence

In order to gain insight in the division between general and specific cyber defence, respondents were asked to answer the question: “Policy often grows from specific occurrences. What is, according to you, an effective division of attention considering general and specific cyber defence?”. P1 answered that general cyber deterrence is more about preventive measures, ensuring risks are well mapped and creating clarity which systems are critical within an organization. You distinguish which data has more risk and you adapt your policy accordingly. Specific cyber defences often involve zero – day vulnerabilities: vulnerabilities in tooling or software that nobody knows about yet. These are often suddenly revealed, and both hackers and defenders (organizations, advisors etc.) race between exploitation and protection. In here, there is a process of measures that you must have in case of a zero day, how to upscale and how to divide priority.

According to P2, a method to divide attention is an estimation of the chance and impact of an incident, and based on that you can determine which measures you prefer to focus on. Risk is then often classified, and plotted within a matrix. This matrix then determines how attention should be divided, based on priority determined by how you assign the x and y axis. Technical vulnerabilities then possess an impact rating which allows for easier decision making compared to ‘organizational’ or ‘process’ aspects. It must be remembered that 99% security means 100% vulnerability. Risk division and identifying the weakest link in a chain must be paired with investments that lower the chance and impact.

P3 supplements that it depends on the type of organization and the risk appetite of that organization. Sometimes for example a network manager spends a lot of funds on cyber security, while their biggest fear is actually a truck running over an electricity pylon, effectively shutting down the power supply to the entire Southern Holland region. It is

important to identify the core of an organization and to prioritize securing that, without resulting to going ‘overboard’ on non-important security measures.

P4 concurs and mentions that it depends on the maturity of the organization. ‘Young’ organizations might be very reactive in their risk control and only respond to incidents. More ‘mature’ organizations spend time and effort looking through a ‘risk control glasses’ about how business is conducted and how to facilitate that. They look at what their mission or vision is and think about what this means considering crime and cyber risk. Then, you want to apply measures, but especially a safety culture within the organization, because there is a maximum to how much measures people can handle and how effective they are. It is rewarding to think in terms of prevention through culture and behaviour instead of reaction through tough measures only.

P5 explains that in general terms, you have to continuously focus on what the effect is that you want or do not want to see. In the incident driven approach however, there is a risk – rule – reflex. Something happens, measures are taken and a lot of steering happens to see if the measures are in fact being taken. The consequence is that people are blinded by working with the measures and lose sight of what the primary desirable effect is. Attention should thus be on the primary effect and repeatedly, through time, attention should fall back upon it, especially as circumstances and context changes occur. The average baseline consists for example of measures thought up by someone of things that could go wrong or either went wrong. The things these measures are meant to solve, can be problematic in two ways. At first, it can solve the problem of one person, but create a problem for another. Second, if a measure is not implemented, to whom is this worrisome? This way, too much focus can be put on problems that have actually aged. These kind of things are very hard to detect in policy or strategy.

4.2.3 Standard versus custom made cyber defence

Keeping standardized security policies, such as ISO’s in mind, I asked respondents to elaborate on their view concerning standardized security policies. I asked them to answer the question: “do you advice cyber policy on the basis of a certain standard or do you prefer to apply ‘custom made’ tactics?”. P1 answered that the preferred method is to apply both. Standardized cyber security models can offer a framework as a base. These standards never fit 100% though and customization must always occur. Especially considering the ‘crown jewels’ of organizations, extra precious assets often involve more customization on top of the standard.

P2 supplements that an important distinction despite the great variety of models available, is that they are either risk or compliance based. Risk based approaches means that you are not just checking boxes according an ISO standard, but you try to see what the effectiveness is of the measures that were taken. This could mean that within the risk assessment for your organization some areas get more focus than others.

P3 states that within cyber security, most work is based on standards, but those standards are enriched with the experience of teams and expertise gained in the field itself. This leads to

best practices. Multiple frameworks for risk management within IS security are then enriched with these practices. Based on their own experience and that of the market, advise is given towards the customers or policy is developed, which should never be static, but remain dynamic.

P4 explains that several cyber standards exist, but often times it is required to return to culture & behaviour as the basis from which an organization should want to operate. There exist cultural models which can be used, that feature cultural elements that are scientifically backed up to occur within organizations. The more 'mature' an organization is, the more these factors are anchored within the organization, and with it the chances of incidents dwindle. Eventually everything is custom made, because organisations to not match on top of each other perfectly. We will always have to think about what kind of culture is featured within an organization, how people operate in this, and then think about what kind of measures fit well.

P5 supplements that standards are well served as an inspiration source as many people have put a lot of thought and work into them, but they will always require tuning before being applied. These standards offer a 'good' way of approaching problems, but that doesn't mean that good things are always done through using it. Applying a certain standard does not equal to solving a problem.

4.2.4 GDT analysis

On the basis of the interviews, we have empirical evidence to suggest that general deterrent techniques are indeed being applied in the field. It would appear however, that many organizations fail to apply these basic deterrent controls or only resort to them after an incident, thus remaining vulnerable in the process. As demonstrated by the interviews, on the level of prevention, it is important that authorization controls are in place. This means that access to both physical and digital assets should be restricted in a well-designed infrastructure. It appears that opportunity reduction is also considered in conjunction with reducing motive, on a general level. An example is the separation of functions and responsibilities to counter fraud before it happens. It is important to understand that different benefits exist for everyone, for example: money, status, and interpersonal relationships. This is in concurrence with the literature review, that mentioned the MICE method (money, ideology, compromise, ego) as indicative for hacker (also insider threat) motivation. Through the interviews, we can acknowledge that it thus remains important to recognize that any digital asset, or physical hardware for that matter, can be considered a target. It would therefore appear, in concurrence with the academic theory, that on a general level, considerable large benefits for eventual insider threat with potential little costs are unwanted. This problem should be approached, by any organization, on a general policy level, and it should strive to either reduce benefits of potential unwanted behaviour, increase the cost, or both.

Increasing the cost is often tied with the detection stage of a security action cycle. Good techniques and proper tooling that detects what you want, can pick up on detection, and offer you handles to plot action against the threat (or incident) are mandatory on a general level. Detection is tied to monitoring and response. Tools that can properly monitor systems are

vital. When looking at prevention, it is known that in cyber security practice it is impossible to always be one step ahead: cyber incidents are going to happen. Therefore, detection is key. If access towards the system is gained, it is important this is detected as soon as possible to enable swift mitigation and control of the damage. Looking back at the principle of GDT, it appears that supervision is a key element in detection and having discernible supervision contributes a lot towards increasing perceived cost and therefore contributes a lot towards general deterrence.

On the basis of the interviews, we have seen that general deterrence is considered at all levels of people, processes, and technology, indicating that the overreliance on technology, such as the implementation of anti-virus, systems, password protection etc., is no longer true for at least cyber advisory organizations. It was indicated though, that most organizations seeking advice do have trouble recognising the importance of all levels, but this appeared to also often include the technology factor itself. When looking at the level of process, having a basic cyber security policy is considered as general deterrence, but this often lacks within organizations. When looking at the level of people, security awareness is indeed seen as a valuable non-technical solution. Further elaborating on the interviews, it appears that general cyber deterrence is indeed about preventive measures, mapping risks, and identifying critical systems within an organization. There is room, and a need, for specific cyber defences, but it remains important that a basic structure remains where it is clear who has which responsibilities and in the case of an incident, how upscaling and priority is being organized.

The interviews indicate that attention has to be divided between general and specific cyber defences however, and even general deterrence is no static subject matter. Risks and threats shift and change, and with it, cyber defences should also. Organizations have to continuously focus on what the effect is that you want or do not want to see. In the field, incident driven approaches with a risk – rule – reflex occur often, but the consequence of this is that a lot of steering happens to see if measures are being taken, causing the loss of sight on the primary objective as soon as context changes occur. Through the interviews, another approach is suggested: risk control tactic, which is not too reactive in nature, and focuses on applying a safety culture with a healthy division of measures. A method to divide attention is to estimate the chance and impact of an incident, via an enterprise risk model, and then classify risk, plot it in a matrix, and determine your attention and budget accordingly. Technical vulnerabilities often lend themselves towards easier decision making rather than organizational or process aspects. It should be noted though, that vulnerabilities always lurk, and identifying weak links must always be paired with investments to lower chances and impact. This in turn depends on the type of organization and their risk appetite: the ‘maturity’ of the organization. Identifying the core of an organization and prioritizing that is vital: don’t lose sight of the primary effect you’re trying to accomplish. On the basis of the interviews, it would appear that it can be rewarding to explore culture and behaviour instead of solely patching security through reactive measures.

Lastly, general deterrence easily lends itself towards more general application of cyber security measures. According to the interviews, these standards (such as ISO17799) can offer a solid framework as a base, but their application is almost never a 100% good fit. The ‘crown

jewels' (most important assets of an organization) and the means of reaching them differ greatly, as such, customization of cyber security measures should always occur. It is important to recognize how general standards are often enriched with experience, expertise, and best practices. This is a dynamic field, and the policies should never be static. Here it is also important to understand that applying a certain standard does not always guarantee the solving of a problem. Certain cultural and behavioural models could and should be applied. Often times, it appeared through the interviews that this insight is mostly shared with the more 'mature' organizations, as these values anchor themselves within the organization.

The empirical evidence thus suggests that GDT is indeed considered in cyber security advisory and fills a very important aspect within the contemporary cyber security field. Many of the academic insights have translated themselves well within the field of cyber security, albeit more within the cyber security advisory field rather than the organizations that approach these advisors for aid. We have seen the importance of deterrence, prevention, detection, and mitigation (or remedies). We have seen that most organizations through general deterrence, indeed try to influence the amount of cost a potential threat would have to pay to get what he supposedly wants. We have seen how policies are often risk and compliance based in their measures, but the knowledge is there that not everything should be 'checking boxes'. We have seen how risk is often calculated through various models, and how action cycles can help in mitigating these threats. Interestingly enough, we can also see how opportunity reducing techniques are being explored within the general deterrence area, which is something ascribed towards SCP within this thesis. It would appear fitting then, to verify once again how GDT is often used in conjunction with other theories. As for the insider threat, the previous chapter has discussed how certain safety nets are considered in deterring certain behaviour from happening, which in essence is general deterrence. Of course, the interviews indicate that the insider threat is not the sole focus point of organizations and therefore general deterrence, as is also indicated in the literature review, approaches techniques for both internal and external threats.

4.3 Social Bond Theory: theoretical preliminary assumptions

The Social Bond Theory studies the commitment to crime if social bonds of attachment, commitment, involvement, and belief, are weak. It seeks to explain social behaviour that does not conform to generally accepted social rule, based on the assumption that a natural inclination towards crime is supressed through strong social bonds. Attachment, commitment, involvement, and beliefs are explored as factors to reduce computer abuse. Social bonds and social pressures can act as informal controls in the form of customs, traditions, norms, morality, or other values, that are implemented by unofficial controlling groups. Attitude of individuals towards their jobs, workspace, colleagues, and general work environment have different implications towards possible delinquent behaviour. How people perceive their actions and the attitude they hold towards non-compliant behaviour heavily influences the actual performance of delinquent behaviour. Loss of belief in social values increases antisocial acts. Beliefs are subjective to influence throughout multiple factors, such as environment, norms, and individual characteristics such as the own subjective norm, or perceived social pressure to perform a certain behaviour.

4.3.1 The natural inclination towards crime

According to SBT, people have a natural tendency towards criminal behaviour, which is supressed through strong social bonds. Respondents were asked to answer the question: “Do you believe that employees have a natural tendency towards criminal behaviour that has to somehow be supressed?“. P1 answered that this was not believed to be the case, without further elaboration.

P2 found this too strongly worded, and believes that there is a correlation between safety culture inside of an organization where involvement is one of the aspects and the eventual behaviour that you see. Motive, means, and opportunity can provide a situation of possible criminal behaviour, and only a minority has a natural urge towards it.

P3 elaborates that in the field, you see that many people actually have a natural tendency to trust other people. A tendency towards criminal behaviour then might make you not trust people, while working together requires a basis of trust. A security & compliance helpdesk can be used to handle notifications when something is off the hook, for example when someone does not act within corporate rules. When looking at people, processes, technology, and governance, these aspects aid to make people aware of security through advancing their policies in a healthy security direction and keep those moving forward in the world of security.

P4 reminds us of the 5% (that always screw up). This does not always have to be intentional, people tend to choose for the easiest route. There might be a natural urge, but that makes us people. We also have an urge to be found nice within our social environment, group conformism is very inherent to people. If people then find themselves inside an environment where a certain behaviour is the norm, then there is a tendency to follow. A nature and nurture story actually.

P5 elaborates that this natural inclination does not have to occur inherently, but it is facilitated by the fact that it is scientifically proven that increasing fraud detection paired with addressing and accusing employees of fraud enables and increases actual fraud. Frequent accusations of fraud somehow forces people to perform the action they are accused of, as they reason it doesn’t matter what they do anyway. This is not a natural tendency towards criminal behaviour, but the result of a ‘toxic’ work environment that the organization can actively promote. Certain individuals that might be able to perform certain unwanted behaviour could be enabled through this toxic organization that pushes their people towards these actions. This diseased corporate culture can stand through time by placing too much mistrust on its employees. If people are trying to do good, but keep getting treated in an inquisitional way, they start wondering why they even try. Group wide accusation of the behaviour of the individual leads toward the wrong kind of social bonding and questioning loyalties.

4.3.2 Application of informal controls within cyber security policy

SBT places a heavy emphasis on the use of social bonds and social pressures, which can act as informal controls, implemented by unofficial controlling groups, that might improve cyber

security. Respondents were asked to answer the question: “Do you see possible application for informal control (e.g. social bonds, social control) within cyber security policies?”. P1 answered that there is certainly room for informal controls and corporate culture is very important here. Agreements on how to address others in certain situations are a must. Informal control within cyber security then shares traits with security awareness questions. How to make people knowledgeable, conscious, and competent in recognizing risks? The top of the organization must radiate the clear example and communicate how important security is. A healthy situation is a situation where everyone can openly speak to each other about security no matter where they stand within the hierarchy.

P2 sees informal controls as the eventual base of a workable work environment. If the field is walled by hard controls and sanction, we find ourselves in a place we cannot work. Very often, it can be noticed that organizations send their people off to do security awareness trainings, or workshops, but you can then notice that culturally speaking something is awry and then these workshops bear no fruit. Motivation to soak up the knowledge and to implement it is required and these are informal things.

P3 explains that informal steering can take lots of forms. Sharing knowledge and being inclusive in that area is one of the prime examples. Lots of these things need to have a formal representation however, because this is often necessary for the larger firms. The most important aspect is delivering a culture based on trust, and through sharing knowledge and intervening at the correct time, we can make the best out of ourselves.

P4 reminds us of group conformism, and explains how the Asch experiments show us that the opinion of an individual can be influenced heavily by the opinion of the majority of the group. It is rewarding to think about how you wish to uphold the desired norm as the group norm.

P5 adds that if the goal is to give people a role within the safety of your organization, measures that enable copy able behaviour can work. Strengthening social bonds through showing how work is done instead of giving people measure to execute enables people to copy this behaviour: copying executional behaviour. If management gives measures but doesn’t apply them themselves, this behaviour will be copied, but this is obviously a bad thing. A culture of fear does not enable this, a culture where others can address issues does.

4.3.3 Influencing employee attitude

SBT theory holds that the attitude an employee holds, towards their job for example, can influence their behaviour towards delinquent behaviour at said job. Different attitude towards non-compliant security behaviour can also have various implications towards security behaviour. To gain insight in ways attitude manifest themselves within cyber security, respondents were asked to answer the question: “ How do you see the possibility towards influencing the attitude of employees against non – conform security behaviour?”. P1 answered that a balance between sanctions and rewards exist. Rewards can then positively influence motivation and enable the visibility of security. Meanwhile, there must always be policy that has clear cut sanctions towards wrong behaviour.

P2 sees vast possibilities. Influencing behaviour can be done through a scientific model that aids in the creation of a safety culture. Behavioural drivers based on prevention, detection, and response aid in in this. When we know the perception of behaviour within an organization, we can test these against the multiple levels that exist within the organization. If these perceptions differ, there is lots of work to do. There are different components that can lead to influencing behaviour in relation to awareness, such as a training side and an exercise side. Within the organization, it is important that management enables the resources to add beneficial components towards the corporate culture.

P3 explains that it is essential for every organization to teach your employees security compliant behaviour. Technology is everywhere and keeps our economy running. To keep this from collapsing, employees must know or be thought security compliant behaviour, yet a lot of branches have not made this switch yet. The future of security lies in security that now has to be thought, becoming a prerequisite for a job in the future. Currently, the human factor remains behind however, which is a problem.

As P4 skipped the question, P5 answered that one of the biggest issues in the security field is the term ‘conformity’, because it implies that everything is about policy compliance. When seeking to influence behaviour, we must be clear in the effects that we want to see and address those, not if we are compliant to a certain measure or not. In their expertise, employees often find smart measures to get to the desired effect. Punctuality tests often confirm that if everyone strictly complies to the rules, the process collapses to unworkable situations. It would thus be wise to steer at effects, not conformity. This input of expertise could be patched in by looking at our current situation. Now, security management makes sure that security measures are all neatly executed: factual compliance. But if you are not thought to ask yourself the question how these measures are going to help the organization, you will never be able to focus on the effect that you want. Measures are now thought up on a level above end user, and implemented downwards in a way that the top level perceives how the end users do their work. This type of ‘checkbox exercise’ does not truly contribute to safety or effectivity, focussing on results and effects does. The organization often consists of a hierarchical structure, but its goals work through a network like structure. Problems that arise don’t follow this network structure, but the old hierarchical ‘rake’, which makes it extremely difficult for the board to patch these problems in an effective way.

4.3.4 SBT analysis

The interviews suggest that the application of social bond theory seems to have found its way within the field, mostly in the form of informal controls that somehow enable a security culture and good work environment. When looking at one of the core principles of SBT: the natural tendency towards crime that has to somehow be supressed (by social bonds according to the theory), the interviews point out that this inherently is often not the case. It was mentioned within the topic of the insider threat, that you have about 5% of an employee base that always screw up no matter what. This does not have to be a natural inclination towards deviant behaviour (it can be however), but can be related towards group conformism, environmental nature – nurture, or simply people choosing the path of least resistance. It is

also worth exploring the way in which a (safety) culture inside an organization correlates between the behaviour that you see. A 'toxic' work environment can build up and can be actively promoted by the organization, either conscious or not, that pushes its employees towards certain unwanted behaviour. Prolonged exposure to this diseased corporate culture spirals down into eventual mistrust, scarce loyalty, and a general sense of apathy towards security compliance. If no strong social bonds can be formed towards the organization, it appears important according to both theory and the interviews, that strong social bonds with colleagues are formed. Compliance enforcement can help when these bonds fail and create unworkable or undesired behaviour, or when the social environment itself creates unwanted behaviour. The interviews do indicate however, that strict compliance enforcement without a safety culture is not as effective as a safety culture that is broadly supported by the organization.

In terms of the possible application of informal controls to reduce computer abuse, the interviews point out that there is certainly room for this and that a certain carry over already exists. Corporate culture is again important here, as this often describes how people should interact with each other. Eventually, informal controls form the base of a workable work environment. If everything is walled off by formal controls and sanction, unworkable situations take place, as exemplified by punctuality tests that show 100% policy compliance leads to process collapse. The most important aspect of informal controls appear to be their contribution towards a workable work culture, and it is important for the management of an organization to think about what kind of culture they want to establish within their business. It is also important, according to the interviews, that management enacts the very measures they apply. Eventually, informal steering can take many forms, this often includes ways of sharing knowledge and being inclusive in that area. According to the interviews, this has to be formalized at larger organizations to ensure this happens, and it is deemed as a necessary process. This is interesting, because it implies formalizing, in some way, informal control factors. We have also seen that group conformism is an issue, this means that making sure the majority of a group feature a desired norm is important, which is something that is thought about in the field, but can also be seen in the light of behaviour that you don't want becoming a group norm, which is where organizations would have a serious problem. What this means, is that SBT theory accounts for group conformism as a controlling factor against deviant behaviour, but in the same way, deviant groups might negatively influence behaviour that was not deviant before. It appears that the beliefs people hold can thus also be influenced by social pressure in a negative way.

One of the most important factors in SBT is that of attitude towards non-compliant security behaviour, and specifically how individuals perceive their actions. These beliefs are heavily subjective and can be influenced by a multitude of factors. We have already seen in the above paragraph how the perceived social pressure can lead to performing certain actions, how about other means of influencing the attitude of employees, such as the own subjective norm? According to the interviews, there are many possibilities. It is important to balance sanction and rewards in order to positively influence motivation, while having clear sanctions available against wrong behaviour. P2 specifically indicates that there exist scientific models, based on

behavioural drivers, that can actually aid in this and are used by P2's organization. In the field, perceptions of behaviour within an organization are actually tested at multiple levels, and if perceptions between levels differ (meaning the different levels have different ideas about right or wrong behaviour) it is safe to assume a discrepancy exists and the organization is vulnerable considering this aspect. This is supplemented by the fact that it is important that management enables the resources to add beneficial components towards a corporate culture. This means, just as we have seen earlier on, that according to the interviews it is both important that management enacts the culture they aim to establish at a broad level, as well as provide the means to be able to do so. SBT theory holds that when beliefs in social values are absent or weak, there is a high possibility of engagement in antisocial acts. Translating this towards the observation of establishing a certain corporate culture, we can see that beliefs are indeed actively attempted to be influenced by for example environment, norms, social pressure, perceived social pressure, and bonds with supervisors or employers. It should be noted however, that this occurs in line with the previously mentioned 'risk appetite' of organizations. According to the interviews, the amount of organizations that actively do so without some form of advisory is extremely low.

Lastly, one of the interviews stands out in looking at the influencing of attitude towards non-conform security behaviour. P5 explains how conformity is actually a big issue, because it implies everything is about policy compliance. In the literature review, we have indeed seen how security compliance (and risk management) are used often in conjunction with most criminology models, and how ISSP's are in place to ensure compliance with security measures, with failing to comply counting as a key threat towards the organization. P5 argues that when seeking to influence behaviour, the effects that we want to see must be clear and addressed, instead of being compliant to a certain measure or not. The point is to not get lost in factual compliance and 'checkbox exercise': where solutions are thought of and pushed down an organizational structure, disregarding end user expertise and leading up to a situation where the desired effect is forgotten and punctuality is tested against a thought up measure, leading to ineffectiveness. It is argued, that eventually, a network like structure is preferred against an old 'hierarchical rake' structure when approaching IS security problems. This is important to highlight, because for example P3 argues that security compliant behaviour is extremely important, and P1 supplements this with the mentioning of a clear cut policy. These are not mutual exclusive statements however, having a clear cut policy is important and balancing rewards and sanctions doesn't rule out that the desired effect is still being focussed upon. Referring back towards SBT literature, and looking at subjects such as attachment, commitment, involvement, and belief, it is clear that in both formal and informal policy creation organizations either are currently aware of, or can be made aware of, academic knowledge and can or are using its availability to improve their IS security.

4.4 Social Learning Theory: theoretical preliminary assumptions

The Social Learning theory holds that crime is committed if a person associates with delinquent peers, who transmit ideas, reinforce delinquency, and function as bad behaviour role models. Differential association, which is the process where a person is exposed to normative definitions that either favour or appal criminal behaviour, makes up for a portion of

this theory, combined with differential reinforcement, which is the idea of expected and/ or realized reward and punishment resulting from behaviour. Criminal behaviour is then learned through communication and a process of expectations that are matched by its behaviour. Attitude about certain behaviour can be formed through association, imitation, and interaction or exposure to sources of learning. A moral attitude that defines an act as 'good', or 'bad', is formed at the hands of this process. Within IS theory, the way through which the social surroundings influence an individual are scrutinized, by assessing the social environment of end users and the possible influences that it can have on behaviour.

4.4.1 Learning, copying, and imitating behaviour

An important aspect of SLT is the learning, copying, and imitation of bad behaviour. Respondents were asked to answer the question: "During the formation of policy, is the eventuality of learning, copying and imitating 'bad' (read insecure) behaviour kept in mind?". P1 answered that this is certainly the case. It is natural to copy behaviour from colleagues. It is important that a code of conduct specifically determines what is expected of people. Corporate culture is important, but very tricky. How do you come to a common agreement of human acting and insight how to work with each other? Cultures clash and change is often incremental. Through audits, interviews and training, people can become more aware and ready for a security environment.

P2 wonders if this currently happens though. Unethical behaviour is often accounted for, and obligation to act upon it exists. It probably doesn't go much further than steering or perhaps addressing your colleagues. Approachability is one of those important cultural drivers. Another important element, that doesn't often show itself in policy, is the 'tone of the top'. If management doesn't exemplify correct behaviour, then its employees copy this bad behaviour.

P3 doesn't believe that this occurs in such a way. Unethical behaviour is often accounted for, and an obligation to act upon it exists. What sometimes happens is that anonymized cases that were treated by the security & compliance helpdesk are posted to show employees what kind of behaviour is wrong. Teach what security consciousness is, and make people aware of the impact of non – compliance.

P4 explains how in general, too little attention is aimed towards culture and behaviour. To understand what behaviour is wishful, and the means to facilitate this, requires a scope of the social environment.

P5 as well does not think this happens. As explained earlier, how can you improve: by creating measures that are copy able. Too much attention goes towards measures that are great from a security perspective, but there is no heed to stimulating copy able behaviour. Too little awareness exists about how 'unsafe' has become a container concept. Depending on who your focus is determines whether you can or cannot do your work safely. In practice, you often see that one side is oppressed to ensure that another side can do its work. If you talk mutually about safety, do both parties have the same concept of what is safe and is this somehow tested?

4.4.2 The influence of a company's culture

SLT holds that delinquency can be passed down by bad behaviour role models and differential association, which is the process where people exposed to norms that favour certain behaviour adapt towards it. There is also the process of differential reinforcement, which is an idea of expected and/or realized rewards and punishment, resulting from a certain exhibit of behaviour. With these influences kept in mind, respondents were asked to answer the question:" What is, according to you, the influence of a company's culture on its employees and how important do you deem this role?". P1 immediately recognized the extreme importance of a company's culture and refers back to the previous answers where organization culture was already mentioned. It is one of the biggest preconditions for acting within a corporation. If you cannot create a certain belief on how business is done and give people the space to participate in this, then you are lost. P2 agrees on how fundamental culture is, and explains it is the basis of the scientific model used for behaviour for a reason.

P3 supplements that this aspect is indeed essential. A culture without trust is a culture without cooperation and no incentive to act within the rules. A sickened corporate culture, whatever the reason might be, will result in unacceptable, sometimes even beyond malicious criminal behaviour. To improve as a team, approachability is so important. A culture of trust to learn from mistakes is vital. P4 also agrees and mentions how culture has an extremely large influence, stating 'Culture eats strategy for breakfast'.

P5 concurs that corporate culture is extremely important. A corporate culture that shows they do not trust their employees will lead to negative effects. A culture of fear leads to a culture of concealment. Distrust within your own employees will lead to behaviour that you do not want. Very little research is done in this spectrum. Lots of research is being done at when people behave criminally, both internal and external, but there are almost no existing works of what these toxic effects are that enable a culture of misbehaviour.

4.4.3 SLT analysis

So far, the interviews are rather ambiguous concerning the application of SLT in the field. On the one side, four out of the five interviewees (P2 – P5) indicate that they are not too sure of the application of learning, copying or imitating insecure behaviour during the formulation of policy. On the other hand, P1 sees that within a code of conduct there is room for SLT theory and corporate culture is already somewhat steered by specifying what is expected of people. Paired with the notion that P1 – P5 all agree that the influence an organization can exercise on their culture is extremely important, SLT theory elements application appears to be scattered and possibly difficult to actually recognize immediately.

Upon closer inspection though, we can see how the interviews do hint at direct implementation of scientific implications made within the theory. Let us at first consider the application of learning, copying, and imitating behaviour within policy formation. Keeping this aspect of SLT theory in mind, some form of formal controls have to be established within policy. P1 recognized how it is natural to copy behaviour from colleagues, thus it is important to have a code of conduct that determines (least) expected behaviour. There is some difficulty

in assessing how this aspect of learning, copying and imitating, which can be seen as the transmission of ideas of bad behaviour, comes forth in the field and how this should be handled by formulating policy, but all respondents did see a way in which this could be handled, thus concluding that even if they answered they did not believe SLT theory to occur within the policy making process, they can actually name direct implementation of it in some forms, which is in line with how P1 perceived that it was certainly possible. We have previously seen how the 'tone at the top' (exemplified correct behaviour on organizational level) is an important factor of SBT, we can now see its reoccurrence in SLT, especially in the creation of a corporate culture that is not necessarily present during policy formation but remains a very important aspect regardless. This 'tone of the top' aspect can thus occur through informal ways, but can be formalized by approachability as a cultural driver. We can also derive its occurrence through the managing of unethical behaviour, and the obligation that can exist to act upon detecting this, which is often formalized in code of conduct, or can be applied through a security & compliance organ. Eventually, this comes down to the understanding that wishful behaviour has to be managed and facilitated somehow.

When looking at constructs such as differential association (exposure towards normative definitions favour or appal behaviour), and differential reinforcement (expected and/or realized reward resulting from deviant behaviour) on basis of the interviews, we can in fact conclude that in both formal (policy) and informal (culture) matters the field is applying scientific insights, albeit the source of the Social Learning Theory itself it not fully mentioned, its application is unquestionable. Though learning, copying, and imitation were not immediately recognized by the interviewees, despite them actually naming direct implications of the SLT theory, the important aspect of culture has been confirmed immediately. Transmission of ideas, reinforcing behaviour, behavioural role models, behaviour learned through communication and a process of expectations that match behaviour, this can all be part of a corporate culture. The influence of culture, according to the interviews, is vital; one of the biggest preconditions for acting within a corporation. All interviewees thus agree that culture is essential, with p3 and p5 mentioning again how a 'diseased', or 'toxic' corporate culture, or a culture of fear, will lead to unworkable situations. Interestingly enough, it is mentioned despite the recognized importance, by P5, that almost no research has been done so far on what toxic effects are that enable a culture of misbehaviour.

Putting this in perspective, we can see that through a corporate culture, certain expectations about behaviour, from both management levels and from colleagues, can arise. Through here, attitude about certain behaviour can be formed, not necessarily only through association and imitation, but also through interaction or exposure to sources of learning, such as the 'tone at the top'. We can therefore conclude that SLT constructs are indeed present in the contemporary field, and it weighs heavily on (often incremental) cultural improvements towards security.

4.5 Theory of Planned Behaviour: theoretical preliminary assumptions

At its heart, the Theory of Planned Behaviour seeks to use the intention towards crime as a factor in predicting behaviour. It is a broad theory that explains the causal relation that

underlies human behaviour, with intention being the key factor. Behaviour is seen as a function of attitude, subjective norms, and perceived behavioural control. Attitude is the degree to which the person has a favourable or unfavourable evaluation of the behaviour in question. Subjective norms refer to perceived social pressures, which indicates that a person could act based on compliance with social demand, depending on what the social norm is. Perceived behavioural control refers to the sense of self – efficacy, which is the perceived ability to perform the behaviour of interest. Behaviour can be broken down into successive elements, and can be analysed in terms of the ability to perform each step in the chain. Within the IS field, the most important addition this theory has to offer is the concern with the ability to perform behaviour, which can influence both the intention and the outcome. This is extremely well measurable by simply scrutinizing how end users perceive their capability to perform a certain behaviour or task, duly noted that the malicious insider might not give away his secrets. It is important to understand that when given a sufficient degree of control over their behaviour, people are expected to carry out their intentions when the opportunity arises. Theoretical models exist that seek to combine this theory with the likes of GDT, SBT, and SLT, referring to these theories as being able to influence the behavioural beliefs (attitudes), subjective norms, and the perceived behavioural control.

4.5.1 Influence of intention

Within TPB theory, the intention towards crime is an important factor in predicting behaviour. We have seen how attitude can influence behaviour in SLT, TPB adds the factor of the perceived ability to perform a certain behaviour, which influences the intention towards it. With this in the back of our minds, respondents were asked to answer the question: “Is there a current role within security policy to influence the intention towards non – conform behaviour to prevent cyber incidents and how is this done?”. P1 answered it is difficult to remove intention if someone has already decided to act, and wonders if there truly is something that can be done about it. A sort of assessment where acting is scrutinized according to corporate standards could shed some light on this. To remove intention though, is something that is worth wondering if it is easy to accomplish. It is important to keep up the conversation with people and see if they remain happy. To keep an eye out for red flags or people who rapidly lose dedication.

P2 supplements how employee satisfaction studies might assist here, to at least map this phenomenon. General dissatisfaction and high pressures or other aspects might reduce the involvement of an employee, and this could lead to them turning to other means to compensate for their perceived shortcomings.

P3 adds that regular terms such as security awareness and training can show people the values of an organization and then you hope that your employees adhere to them. These workshops focused around awareness might drive them to change their behaviour accordingly and give them the insight that security within their own organization is important.

P4 sees the attitude of intention as one element, and motivation as the other. Both of these are influenced through the (social) environment, and this environment influences even more. The sphere of influence within an organization can exceed its boundaries, and it is interesting

to see how behaviour that is wish able is taken back to other spheres, to see how for example people deal with sensitive corporate data back at home.

P5 sees a development of interest for this subject, but there are only a few parties actually at work. It is fairly new, but a very important aspect worthy of attention. Problems arise however, how to measure intention and how will you detect and organise this? To implement this in an organisation will be tough, but do – able.

4.5.2 The connection between intention and execution of behaviour

As TPB seeks to explain the causal relation between human behaviour and intention, and as intention, according to this theory, can be formed accordingly with the ability to perform certain behaviour, respondents were asked to answer the question: "What does the role between intention and actual execution of behaviour look like when considering accidental and malicious incidents?". P1 explains how important this behavioural science theory in the field is. Most people are reluctant to act towards their intention. Considering the insider, there are many people who are dissatisfied with something, who might think about doing something wrong, but the question remains if they will act. At the same time it is hard to measure this, because corporations are reluctant to provide this sort of data. The intention and acting upon it is confined to how measurable and testable these are, it can be rewarding to look at the definition of the insider as those with malicious intent.

P2 elaborates that as far as accidental and malicious incidents go, both can occur. Within the cyber domain, accidental incidents often involve employees doing something because they were not paying attention or because it looked easy, or because they actually have no knowledge of the possible impact and consequences. Intention also plays a part, but the malicious incidents are outnumbered by accidental ones. It is difficult to measure, because once you get away with it, it doesn´t appear within the statistics.

P3 goes further into depth and elucidates how intentional wrong behaviour has an intention lurking behind it, but considering accidental behaviour, there does not have to be a strong connection with a wrong intention. Often, the intention is not wrong, but the behaviour is. A case can be made that the intention is often to help colleagues, but in the process rules are broken. Mystery guest and social engineering assignments often prove these factors to be true. Unintentional wrong behaviour thus often springs from good intentions, that eventually spur a risk to the organization. This has to do with what someone´s role is within the organization, and if it is their job to think from a security perspective. Making mistakes is humane, it is the insider threat, but it is not always conscious. Even so, people should be stimulated to show the correct behaviour.

P4 concurs that it is difficult to prove whether something is intentional or not. Much of our behaviour is somehow forced, perhaps because it was at that time desirable, and in hindsight we might claim it to have been on purpose. This is a matter of admitting that something was intentional. Unintentional incidents occur often because people were not paying attention, or perhaps were never attended at their wrongful behaviour by others or they were given too

much opportunity to perform this behaviour, perhaps even encouraged by others or perhaps out of ignorance and boredom, just to see what would happen. Eventually, mistakes happen.

P5 supplements that the difference between geniality and stupidity is that there is a limit to geniality. Those accidental incidents will never cease. Intentional incidents are often an accumulation of rights. Big incidents happen when people hop from function to function, retaining their rights, increasing the opportunity to behave badly and eventually this is a basic security policy fault.

4.5.3 TPB analysis

Considering how TPB occupies itself within the IS field to study the influence of intention of behaviour, according to the interviews, its application is rather ambiguous. On the one hand, interviewees indicate that intention is difficult to measure, assess, and gaining insight in the relevant data is problematic since most organizations either don't know how to measure this, or refuse to share relevant data. On the other hand, the cyber advisory field is currently vividly applying TPB constructs, with P5 even mentioning that influencing intention itself, which is considered to be the hardest part of TPB by the other interviewees, is rising in both interest and development, albeit only by a few parties at work and the concept being fairly new.

At first, let us consider the subject of attitude, which is the degree to which the person has a favourable or unfavourable evaluation of the behaviour in question. As we have seen in the chapter on insider threat (4.1.3), and according to the interviews on TPB, if people are unhappy or highly put under pressure, attitude might shift towards malicious or uncaring behaviour fast, which from a security perspective is problematic. In the SLT analysis, we have seen that attitude can be influenced through the social environment. In the SBT analysis, we have seen that attitude, specifically towards non-compliant security behaviour, is heavily subjective and can be influenced by a multitude of factors, such as perceived social pressure, own subjective norms, tone at the top, social environment, tone at the top, toxic or healthy corporate culture, and of course social bonds. In TPB, we see that social demands or a current social norm can influence intention, and this influencing is done through perceived social pressures known as subjective norms. Seeing as how in SLT and SBT these perceived social pressures were deemed as important and present in the field, the same can be said for TPB.

The interviews mention stimulation of the correct behaviour, and in general more security awareness, as a foremost counter towards both intentional and accidental security incidents. Accidentiality and subsequently intentionality are difficult to measure and assess however. Removing intention might pose problematic, but keeping the subjective norms, which can indicate that a person could act based on compliance with social demand, depending on what the social norm is, in check can be done through keeping up 'the conversation' with people. Through employee satisfaction studies for example, an eye could be kept out for red flags that indicate people rapidly losing dedication. In general, security awareness and training can keep people in line with organizational values and could change behaviour. We can see here how attitudes are sought to be understood and perhaps influenced.

When considering the perceived behavioural control, or sense of self – efficacy, which is the perceived ability to perform the behaviour of interest, an interesting link to GDT occurs. General deterrence is implemented, broadly speaking, to deter certain behaviour from happening. GDT therefore directly tries to affect perceived behavioural control: if a person does not believe being capable of executing a certain behaviour, because GDT makes that person to perceive they are either unable to or won't get away with it, the behaviour might not occur. This is concurred by the interviews, but there is a problem of assessment, especially considering maliciousness and accidentiality. From the interviews, it proves difficult in the field to prove whether something is intentional or not, and that accidents are probably always going to happen, but the most interesting aspect is that according to at least P2-P5 accidents can happen even with a good intention behind them. Wrong behaviour can thus spring from good intentions, and even good intentions still pose a risk towards organizations.

This also implies that most of the behaviour is somehow steered, and sometimes the perceived ability to perform behaviour and the eventual behaviour that occurs does not line up. This also has to do with opportunity, as the interviews indicate that following through on intention does not only stem from intention, but opportunity as well. Though this is treated more in depth in the chapter of SCP, it is interesting to look back at how TPB aligns with GDT, and perhaps how GDT should disable opportunity to perform unwanted behaviour. Especially P4 stated how when given too much opportunity, or through thorough encouragement by others, mistakes or intentional wrong behaviour might happen, and this is also considering ignorance and boredom, as these should be at least apprehended in a basic security policy according to P5, and can therefore be seen as undesired opportunity towards wrong behaviour.

Eventually, TPB theory assumes that when given a sufficient degree of control over their behaviour, people are expected to carry out their intentions, especially when the opportunity arises. According to the interviews however, behaviour can occur without a certain intention behind it, people might not act out on their malicious intention for whatever reason (if deterrence does its job, they might perceive to not get away with it, or perceive there is nothing to gain, or perceive the consequences and deem it not worthy, etc.), or people might carry out their intention even without opportunity.

It would thus appear that the importance of TPB's theoretical contribution has not escaped the field's grasp, but there is a recurring problem of measurement, available data, and the relatively difficult concept of intention being assessed, though attempts are being made. It is safe to conclude on the basis of the theory and the interviews that although difficult, academic TPB concepts are being applied in the field and it is worthwhile to invest in continuing to do so.

4.6 Situational Crime Prevention: theoretical preliminary assumptions

The core of the Situational Crime Prevention theory revolves around opportunity as the focal concept, where the occurrence of crime is based on a combination of motive and opportunity. The characteristics of a crime become just as important as the person who commits it. Instead of centering on psychological, biological, or social factors, this theory regards crime as an

event, and highlights it as an ecological occurrence motivated by opportunistic factors. It shares traits with the rational choice theory, claiming that the crime should be viewed from the perspective of the offender with a focus on thinking, decision making, and opportunity. Also sharing traits with GDT, cognitive abilities are used to structure choices based on the perceivance of benefits or costs. With the rational actor in mind, questions of accountability and responsibility enter the playing field. Implementation of opportunity reducing techniques can impact their environment through its design, management, or manipulation, and aim to either increase the effort and risk of crime, render crime less rewarding or excusable, or reduce any provocative conditions. Moral during the decision making process is also considered, and can be viewed in light of being supressed to nullify eventual feelings of guilt that might inhibit certain behaviour.

4.6.1 Provoking and hindering conditions to security behaviour

Seeing as how opportunistic factors are an important part of SCP theory, conditions that can potentially either provoke or hinder non conform security behaviour are an important aspect. To gain insight in how certain conditions can alter behaviour, respondents were asked to answer the question: “Will conditions that could potentially provoke or hinder non conform security behaviour be taken into account within cyber policy?”. P1 answered that the insider threat rises, because a diverse cast of people are working in your systems. The question arises, what and who is an insider. It is possible that someone suddenly becomes an insider. By performing an assessment about who needs what data and who needs access to what part of the system, you can determine the terms and conditions that need to apply. These policies combined with risk assessment feature measures that are taken to reduce opportunity.

P2 supplemented that in the larger organizations you see that opportunistic factors are reduced as much as possible and authorization and logging are in place to reduce the chance of unwanted behaviour up to the point where if it occurs it is at least documented. At the newer, smaller organizations, this is based on trust, and this fails in practice especially when third parties start to get involved. Opportunity driven elements should be at least addressed in the policy.

P3 explains how their security policy has four axes: people, processes, technology, governance. It also consists of some other elements: predict, identify, prevent, detect, respond, recover. The most important job is to identify your ‘crown jewels’, and secure these assets. There are technical and organizational elements to prevent people from showing non – conform behaviour, this is where their security portfolio is grafted on.

P4 does believe these conditions will be taken into account, and explains that there is a lot of attention to the possession and authorization of data, and what this means considering the risks involved. Who is capable of doing what within the organization? To think of certain measures to prevent unwanted behaviour is good, but it emphasizes the negative parts. You could also think about how to improve wish able behaviour. Sanctions versus rewards.

P5 explains how segregation of duty is important here. The person that enables payment processes should not be able to control them as well and handle the payments. Sometimes the

business side of a corporation has this nicely separated, but then the IT side only has one person for the entirety of the task and then opportunity arises at the technology side. When translating the business requirements to the IT systems, sometimes risk is unwillingly created. Even if the policy accounts for this, the fine tuning can still create holes. The business – IT line has to be in order to be able to spot these kind of weaknesses. If an organization is troubled by an ICT incident, this indicates that there already is a problem within that line. There is a simple test called 'black swans & perfect storms'. Only incidents that weren't known beforehand and were literally unpredictable, known as a black swan, should be able to cause crisis. Alternatively, an accumulation of factors that will lead to incidents is known as a perfect storm, should also only be able to cause a crisis. Everything between these two extremities causing a crisis means that your risk management is not up to par.

4.6.2 Roles within security policy

As SCP takes the characteristics of a crime into consideration, with a focus on opportunity, opportunistic factors that may influence behaviour are taken into account. Though the amount of factors that can influence opportunistic behaviour is non exhaustive, within the literature review we have seen elements that aim to either: increase the effort and risks of crime, render crime less rewarding or excusable, or reduce provocative phenomena in the immediate context. As such, respondents were asked to answer the question: "Do the factors, 'effort, risk, reward, provocation, and excuses' have a current role within a security policy?". P1 answered that the more effort someone has to put into an action to circumvent security, the better this is for security. Risk is always important to consider within a policy. Everything depends on the traditional enterprise risk that determines the amount of focus a subject gets based on occurrence and potential harm. For the perpetrator, risk is often small in cybercrimes because of its anonymity, making it very appealing. Rewards work in two directions: the hacker sees it as something interesting, such as money or reputation. For the organization, this is a loss. Risk assessment looks at certain risks involved and determines their impact and the amount of loss the organization can sustain. Provocation can sometimes be used beneficial, for example inviting ethical hackers to help you improve your defences by offering them money. Excuses are hard to conduct policy on. Perhaps through awareness, bringing people up to date on what the policy is. Often, corporations offer some sort of security awareness programme, but in practice you'll see they don't really learn a lot. Generic excuses also occur in the sense that people try to shift responsibility away from them, claiming for example that it is not up to them but up to the IT department to prevent a phishing mail from entering their mailbox.

P2 sees a way within policy that steps are being taken to increase the effort required as an attacker, together with increasing the risk. A layered form of security can be an example to increase both. Considering rewards, there are various options available. Division of assets and internal access towards 'crown jewels' is a good start. Provocation can be seen in the light of an exercise that we sometimes do: a mystery guest. Through social engineering we want to find out how far we can go and where the risks truly lie. P2 did not really recognize excuses to have a role here. P4 certainly sees the first four factors being present in current policies, but also sees excuses as a difficult one.

P3, in general, advises a response & disclosure policy. If someone hacks an and doesn't deal too much damage, and notifies the organization before going public, they can reward these efforts to improve their defences. You can always start judicial action, but if you recognize that this is a learning moment you can use this to your advantage. Reward and excuses are major contributors here. Effort, risk and provocation are not directly recognized. The most important part is looking at your core, most important assets, and design a security perimeter around that. Considering the insider, CERT (Computer Emergency Response Teams) can keep a company safe and respond to potential malicious behaviour. This behaviour can be spotted by the proper tooling, or from reports of employees who suspect something. With this, comes a policy that features increased effort for sharing data. There are also other examples of policy, such as the clean desk policy, to prevent incidents from happening. There is also a lot of informal control, to make people aware of these security policies, such as pranking people who forget to comply towards a certain policy. This kind of informal banter is not supplied from management, but from bottom up.

P5 explains that if we look at social engineering, these are major factors at play. It is difficult to say if we can find these factors within a tight policy though. It could prove to be difficult to have an effective policy implementation here. It must be said, that finding out what the actual damage of insider threat is, is an interesting question. Does it increase? Decrease? Are certain sectors hit harder than others? What is the relationship with policy? This kind of information is difficult to get a grasp of. Where exactly lies the separation between an insider and an outsider? Is the guy who got fired but still had credentials in insider or an outsider? What is often portrayed as a hack is in reality a person or group of people that has access to a system and is somehow motivated to do something with it.

4.6.3 Accountability and responsibility in cyber policy

As SCP shares trait with the Rational Choice Theory, which assumes that people's behaviour is based on rational decision making and people are therefore accountable for their own actions, respondents were asked to answer the question: "How are the factors of accountability and responsibility being dealt with in a cyber policy?". P1 answered shortly that these are legal questions which are often already baked within policy.

P2 supplemented that sometimes responsibilities within incident response organizations or at management level are not clear cut. This means that during crises, it is unclear who has the mandate to 'push the button' and take everything offline. These responsibilities are not well agreed upon and having a discussion about this subject during a crises is too late. Therefore, it is important to know who is accountable or responsible for what and if you do not know, it is essential to fix this quickly.

P3 adds that within their organization, everyone is responsible for their own data and how they handle it. You are accountable as an employee, and have your own personal responsibilities. You are tested and judged for this. If we look at the market, there is still lots of room for improvement on this topic. It is absurd that AVG 15th of May 2018 causes such a stir up through entire business Holland, while this is something that should have been taken care of a long time ago. Parties should start thinking about the nature of the assets that they

have and start to be responsible towards that in an appropriate matter. As a whole, this does not happen enough.

P4 mentions that current day, especially CIO's are accountable even if they did not do something themselves. They are responsible for what happens below them. Employees however, do have the responsibility to handle data in a responsible matter.

P5 sees how these terms are used within policy. What are your responsibilities? It is important to look at what your goals are and how you want to realise those goals. If someone is made responsible for realising those goals, the risk is not being able to realise those goals. How does the responsibility that this person gets match the goal that he must achieve? Failing to invest in the responsibilities required to reach the main goals leaves vulnerabilities in its wake and effectively created a risk. This might seem paradoxal, but a policy that does not check the effect of the goal, but the effect of the measure ends up creating an inherent risk, despite the fact that the policy was there to prevent the risk from happening. When different parties meet and discuss about risks and responsibilities, often they are talking about different kinds of risk. In generic terms, it must be obvious if the responsibilities and risks match, they have to be specified.

4.6.4 SCP analysis

SCP revolves around opportunity and motive, with crime being viewed as an ecological occurrence motivated by opportunistic factors. In the literature review, we have seen how prevention of certain behaviour is sought after by influencing these opportunistic factors, such as by increasing the difficulty of executing criminal behaviour, increasing the chances of criminal behaviour being detected and punished, reducing the perceived benefits of criminal behaviour, reducing provocations or removing any form of justification for criminal behaviour.

In the interviews, we have seen how provoking or inhibiting conditions towards security behaviour can be taken into account within cyber policy. Policies can be formed with the help of risk assessments to see which measures should be taken to reduce opportunity. This of course depends on the scale and maturity of organizations, and their vital assets. As we have also seen in the chapter on GDT at 4.2.2, especially larger and more mature organizations want to reduce opportunistic factors as much as possible, and ensure that authorization and logging are in place to reduce the chance of unwanted behaviour, or at least be able to document it if it does occur. Eventually, the interviews seem to indicate that through the possession of data and the risk management involved there, organizations have to think of measures to prevent unwanted behaviour. Interestingly, P5 is the only interviewee here who mentions business and IT alignment and how risk management between the two extremities of perfect storms and black swans should be up to par to prevent incidents from happening. This is in line with the earlier statement by P5 in 4.5.2, that 'accidental incidents will never cease…increasing the opportunity to behave badly…is a basic security policy fault'. This is also in line with P2, who mentions in 4.2.1 that incidents are going to happen anyway, and arguments that the main point is that if prevention fails detection should be up to par. Another interesting approach of provocation is mentioned by P1 and P3: where provoking attackers to

execute their behaviour can act in your advantage. They explain how these efforts can be rewarded and used as a learning moment, to patch up the defences. This can be done as suggested by the interviews by either contacting ethical hackers to probe your defences, or to do business with black or grey hats who before going public contact your organization. This somewhat resembles how P2 mentions mystery guests as part of provocations.

As for the opportunistic factors themselves, the interviews show that increasing effort and risk, reducing reward, lowering provocation and rendering excuses less available are somewhat presented in modern day policies, though not all interviewees recognize all these factors, with P5 doubting (but not being sure) if these factors can actually be found within a tight policy. Let us look at the factors presented in the literature review one at a time. Increasing the effort someone has to put into an action to execute criminal behaviour (or circumvent security) is considered to be a worthwhile security measure. Increasing the risk someone has to take to execute criminal behaviour is often paired with increasing the effort. Within the interviews, we can see how risk is always an important factor to consider within a policy. Risk determines the amount of focus a subject gets, based on occurrence and potential harm (as we have seen in the literature review in standard risk enterprise models). For perpetrators, having a low perceived risk of getting caught makes it interesting to perform criminal behaviour. Increasing risk can be as simple as enabling layered forms of security, increasing detection and response tooling and policies, and generally having a sound security policy. Reducing rewards, according to the interviews, is something that should be done mandatory, but can be applied in a multitude of ways. The rewards of an attacker are often valuable assets of an organization. The organization can therefore choose to somehow use division of assets or restricting internal access to assets to make breaches less rewarding. In another way, it has been mentioned before how proper monitoring and response can make the crime also less rewarding, by increasing detection and mitigation. As we have already discussed provocation in the former paragraph, where it is indeed recognized as a valuable factor within security policy, though not directly recognized as such by P3 and P5, despite P3 actually mentioning having a response & disclosure policy that rewards hacker efforts when informing the organization without going public which can be seen as a representation of provocation within policy, I will refer back to that paragraph instead of elaborating on it here. As for the final factor, excuses, this is one of the least recognized factors considering its implementation within policy, but it is recognized as an occurring theme within the field. Generic excuses can happen when people try to shift responsibility away from themselves, but excuses also happen after incidents which should be approached as learning moments instead of dodging responsibilities according to the interviews.

In the literature review, we have seen how SCP shares some crossover with GDT as cognitive abilities are used to structure choices based on the perceived benefits or costs. Within SCP, we see how motive and opportunity are used to structure choices, which has a focus on opportunity. Within GDT, deterrence is sought after by influencing choices in such a way that certain behaviour (criminal) is prevented, which has a focus on deterrence through motive. In chapter 4.2.1 we have already seen how P3 mentions that opportunity is one of the major grounds of criminal behaviour, and how separation of functions and responsibilities as

part of GDT can work to reduce opportunity. This is concurred by P2 in chapter 4.3.1, where motive, means, and opportunity are mentioned as a situation of possible criminal behaviour. In chapter 4.5.2 P4 and P5 also mention how too much opportunity can result in wrongful behaviour and security incidents. While the interviews on the topic of SCP do not mention GDT itself, they do mention deterrence as a way to reduce opportunity and/or opportunistic factors, and having proper monitoring, logging, and response in place, as well as mentioning the crossover with SCP earlier in the interview as demonstrated in the sentence above. This is in line with how according to the security action cycle, if deterrence fails, detection should be up to par, and also confirms that deterrence is there as a disincentive to behaviour, be it by removing motive, or opportunity, or both. Another interesting note is the mentioning of informal factors (also not present within the policy) as a way to reduce opportunity, which implies a connection with SBT and SCP.

As people are expected to carry a certain intention towards certain behaviour, and they execute this behaviour as soon as the opportunity arises, we can see a perspective of the rational actor, who is accountable and responsible for their behaviour. According to the interviews, accountability and responsibility are indeed factors that are dealt with within a cyber security policy and if not these should be baked within policy. Within the interviews, we can see however that responsibilities within organizations are not always clear cut, which means that during crises it is unclear who has the mandate to act, which means that as far as accountability and responsibility goes organizations in the field sometimes have some serious problems in their policy that should be addressed. Within the organizations, employees often have their own responsibilities and accountabilities, but the interviews indicate that this very basic principle doesn't happen enough in the field. An interesting notion by P5 is that in concurrence with the other interviewees that these terms should be used within policy, it is important to understand that when talking about goals, measures, and risks, different parties often talk about different kinds of risk, and in generic terms, responsibilities should match this risk accordingly, which can produce problems.

After TPB's and SLT's more doubted application in the field, SCP seems to be recognized far easier by the interviewees, though some of the opportunistic factors were not immediately identified. It is safe to conclude however, that in line with the literature review, SCP has indeed proven to benefit the field through its application and is indeed used within the field in conjunction with other criminological theories to provide opportunity reducing techniques.

4.7 Respondent's thoughts on improvements in the field

Having treated the criminological questions, one final question remained where the respondents were asked: "In your opinion, where is the biggest area of potential growth in the field of cyber security? In what area and in what way?". This was asked to conclude the questionnaire and see if any topics remained to be discussed. Through these answers, more insight in what is currently playing in the field is possible, and a better comparison of academic insights and in the field occurrence can be made.

P1 answered that integration between all components of an organization is important. There are generic IT risk management, system rigging, continuity problematics, and security,

both technical and the measures that you take. On top of that, we have generic risk management, enterprise risk management, exposure, regulators, AVG, GDPR, privacy issues, how do we get all of these together? How do we get one clear picture of the impact of cyber in this whole area? Despite business and IT alignment, cyber is not yet part enough. Many organizations know what they have to do and have a professional eye on what needs to happen, but to put all of it together, to ensure that IT departments, security departments and the business as well cooperate as one? That remains a challenge.

P2 answered that many organizations do not shed enough light towards human factors compared to other measures that are being invested in. The improvements for the human factor are often hard to measure. Long term changes in a cultural aspect remain difficult. The difficulty in measuring improvements, compared to technical improvements which are measured easily, makes it hard for managers to argument in favour of investment in this area. Despite short term effects being hard to measure or notice, P2 estimates about 8/10 incidents to have a human factor perspective towards it. It is important to realise that the human factor is the first layer of defence. Very rarely can you actually hack a server through the internet, the human route is easier and often shorter. Not enough attention is spend towards this human factor, especially risk groups within organizations. These risk groups consist of people who have direct access to sensitive data. From a cyber or fraud perspective, these people should be trained extra, according to P2, but this does not happen in practice. These people are often tagging along with a broad program that is arranged, but they should be viewed separately as they carry more risk with them.

P3 at first believes security should be structurally featured in both basic and higher education. Awareness programs and workshops should be crafted and made part of the general curriculum. Secondly, basic controls offer the potential to make so much right. Parties claim that they have no money for basic controls, but some basic controls do not cost money. A clean desk policy for example is costless, but will prevent data from lying around. There are human basic controls, but also basic security controls and technical controls. Think of an anti-virus, a firewall, a small vulnerability test for your website. It does not have to cost much, but it will prevent all your hardware from becoming a botnet or having your data sold all over the internet.

P4 believes we can gain the most traction by investing in culture and behaviour. Security in many organizations is performed by either security people or technicians, always with an IT background. There are no psychologists, nurturers or criminologists working in the field, while P4 does believe that the influence of behaviour can have much more effect than technical measures. P4 would like to see the security department to have a more diverse background including sociology or psychology and that these people get to add in their knowledge, also from a policy point of view.

P5 believes the way forward is to reason with involved parties and specify when something is going right and when something is going wrong: effectively stating when a goal is reached or not. Success is defined by your capability of ensuring the primary goal is hit. This what risk management should be about: during changing goals and multiple dependencies, can we still

be successful? Right now, we think of what can go wrong, we take measures, and we put a lot of effort in thinking if these measures are executed well enough. We no longer concern ourselves with achieving the goal. Dependencies are dynamic, goals are dynamic, the way through which we cooperate to realise the goal is dynamic, and meanwhile we remain static on risk management drooling off following compliance rules. To realise that the goal of one is not the goal of the other, and to realise that therefore the risk of the one cannot be the risk of the other is an enormous gain. Groups grow in size, the same for the stakeholders, in order to streamline this slow process of analysing every single thing that can go wrong, we would be better off to think about relating a group towards their goal and to determine if the goals and risks even match. It is important that we determine fast if multiple stakeholders are even relevant to each other. We have the methods to do this, the biggest problem lies in getting people in the same thinking modus. If people stop believing in this functional 'rake' of organizations and start thinking and looking at the way business is conducted, then security and risk management can start to see how to truly facilitate the business. Security and business are separate models, but should be looked at in conjunction. If you forget to put both models on the same measure, either very unsafe situations occur, or an unworkable environment emerges. Bringing together more and more parties with different interests is going to bring about conflict, it is important that we oversee this and keep the interests and requirements sharp. Different divisions should be integrated, which is very hard. People who do not have a shared expertise and knowledge between fields, because nowadays everything is so specialized, result in mismatches. Translating the IT and the business, is hard, costly, time consuming, but necessary to remain operationalizable. So the biggest room for improvement remains to realise if you are helping people to do their job, or are you helping security explain to people how to do their job?

4.7.1 Concluding remarks analysis

P1 mentioned how the field struggles with integration between all cyber security components of an organization. Despite business and IT alignment, cyber security is not yet part of the big whole. In the literature review, we have discussed how organizations can struggle between technological, organizational, and social factors. This description by P1 matches that image of organizations struggling with one of more of these factors, and it is perhaps worrisome to see that in the field this area is still considered to be an area of potential growth and an overall challenge, instead of it being an area actively engaged in improving. This is concurred by P4, who believes most traction can be gained by investing in culture and behaviour. P4 mentions how security in many organizations is performed by either security or IT people, and is lacking psychologists, nurturers, or criminologists. This happens despite the influence of behaviour being perceived as more effective towards an organization's cyber security, confirmed by the thesis' literature review and the interviews. It would therefore appear to be a good practice according to P4 for organizations to invest in a diverse background for the security team, including sociology or psychology, in order to add more knowledge.

P2 answered that organizations often fail to understand the importance of the human factor compared to other measures that are being invested in. When looking back at the literature

review, this is very much in concurrence with academic insights. The classic image of an overreliance on technological measures while forsaking human or organizational approaches appears to be appropriate. P2 does explain why this is the case, which is something that has not been treated as much within the literature review. I explained how often times risk management is used to balance risk acceptance, budget, and potential loss within organizations. P2 explains here how a difficulty in measuring cultural aspects and cultural improvements adds fuel to the fire. Short term effects in this area are hard to measure or notice, this in turn makes it hard for managers to argue in favour of investment in this area, despite the human factor perspective being overrepresented as a cause for cyber incidents. It is also important to notice how P2 indicates that only on rare occurrence hackers manage to get to a server through the internet, leaving the human route as easier and shorter, as also indicated by the literature review. This indicates that the human factor should indeed be considered as the potentially weakest link in the cyber security chain, based on the context per organization of course. We can also see how it is important to understand that the human factor is often the first line of defence. Throughout the thesis, on multiple occasions, has it become clear that the human factor should be considered as a primary focus area. P2 indicates that in the field, organizations still fail to recognize its importance.

Another interesting topic brought up by P2 is how from a cyber fraud perspective, people who have direct access to sensitive data are often not trained accordingly. In the literature review, we have come to the conclusion that security and awareness training is one of the greater non-technical solutions for cyber security, and the interviews have confirmed this as well. If organizations fail to recognize more special categories of users however, as P2 indicates here, an argument can be made that these solutions are not used up to their full potential, or might not even be effective. Considering security awareness training, P3 also believes awareness programs and workshops play an integral part in improving cyber security. P3 believes these programs should be made part of the general curriculum, and perhaps even be structurally featured in basic and higher education.

Secondly, P3 mentions how in P3's experience many organizations lack even basic security controls, often claiming that they have no budget available. This is interesting from a number of perspectives. At first, P3 explains this problem does not only concern the human factor, but also technical controls. This is counter intuitive, as both the literature review and the interviews have established that most organizations overemphasize on technical controls. However, the organizations lacking these technical controls as well, as indicated by P3, seem to lack any form of basic controls at all, indicating that security is no priority in those organizations. This is very worrisome, considering these organizations do possess either hardware, software, or data that could be valuable to attackers. Another perspective that is interesting about this phenomenon, is that often very basic security controls do not have to cost much, or cost anything at all. Which leads towards the next perspective: do these organizations have a budget available for incidents? If not, do these organizations have their risk assessment in order? This indicates that lots of organizations are not mature enough yet, which by itself is fine, but this also implies compliance to national laws are not in order, which poses a threat.

Looking at organizations themselves, P5 mentions how an area of improvement lies in more realistic goal achievement and adjusting cyber defences accordingly. This topic is about looking more at risk management and realising what it should actually be about. Right now, during changing goals and multiple dependencies, many organizations look at things that can go wrong, taking measures, and putting effort in measuring if compliance to these measures is being met, but actively looking if the goal is being achieved loses priority. The way P5 describes this, is by stating that as dependencies and goals are dynamic, the way through which cooperation is assured to realise the goal should also be dynamic. This is however not the case in the field, as mentioned by P5, and organizations remain static instead of dynamic on risk management, and 'drool off' following compliance rules. In the literature review we have seen how a compliance based approach is often used by organizations to offer procedural measures for cyber defence, and ensuring compliance with security measures. As indicated by this interview question however, if the organization steers away from the primary goal and focuses solely on compliance, these compliance measures could become less effective than their intended goal. As indicated by P5, to realise the goal of one is not the goal of the other, even in the same organization, and therefore to realise that the risk of the one cannot be the risk of the other, is an enormous gain.

In practice, this translates to goals and accompanying risks not having an even match. According to P5, this problem lies in getting people in the same thinking modus, which is hard due to the functional 'rake' of organizations. This means that when looking at the way business is conducted, security and risk management often claim to facilitate the business, but in reality, only solve their own problems. P1 concurs this when discussing P1's topic as well: despite business and IT alignment, organizations struggle to combine efforts of different branches within their organization. P5 indicates that it could prove to be more effective to consider which stakeholders have which interests, and to see if multiple stakeholders are even relevant to each other. Security and business are separate models, but should be looked at in conjunction. As indicated by the interviews before, and now yet again by P5, if you forget to put both models on the same measure, either unsafe situations occur, or an unworkable environment emerges. In practice, bringing together multiple parties with different interests is going to bring about conflict, which makes it all the more important that the interests and requirements remain sharp. P5 indicates this is further problematized as everything today is heavily specialized. Without knowledge between fields, it becomes difficult to enable this proposed integration where business and IT models are considered when coming up with measures, and parties only resolving their own problems, but not their shared problems, remains a common occurrence in the field.

Chapter 5: Conclusion

In this chapter, I will answer the research question: through a multi-disciplinary approach comprised of information system security theory and criminology models, to what extent are contemporary scientific insights regarding cyber security with a focus on the insider threat applied in organization's policies? I will summarize the results of the previous chapter and structure them in such a way as to draw a partial conclusion per subject, and thereafter add the final conclusion. This is followed by a brief mention of recommendations for future research.

5.1 Extent of insider threat representation in the field

Overall, academic insights indicate that the insider has the potential to cause more damage than an outside attacker. Empirically, the interviews have indicated that this is indeed the case. However, it should be noted that opinions are divided on the perception of where the biggest risk lies, which is dependent on the scope, domain, and sector of organizations. It is therefore reasonable to conclude that the potential for more damage than an outside attacker is there, but in practice, the insider threat does not have to be the biggest actual threat an organization can face, depending on the context per organization.

Comment [SW1]: Dit klinkt erg tegenstrijdig

It should be noted though, that as according to both the academic theory and the interviews, the insider threat is rising, due to multiple reasons. At first, there is an increase in third and fourth parties in the business, which leads to more privileged insiders and therefore more opportunity for people to abuse their privileges, as well as opening up to more ways accidental incidents from the inside can occur. Secondly, the interviews indicate that most focus is aimed towards external threats, which makes a growing number of insiders problematic as both internal and external threats are equally worth consideration. Simply put, with a growing insider threat, and no shifting focus away from external threats, the insider risk grows. Thirdly, the interviews also indicate that many organizations struggle with basic cyber security foundations, which leaves cracks in fundamental aspects of the organization, reducing the ability to withstand both external and internal cyber-attacks. As indicated by the interviews, this reduced resilience also means that organizations will struggle during and after an incident, and this could even possibly lead to an organization never recovering. Another factor as indicated by the interviews is that possibilities exist where external threats attempt to recruit insiders for fraud operations with shared interests. This occurrence of blurring boundaries between the internal and external side makes it difficult to remedy these insider threats. The interviews indicate that many organizations try to muffle inside incidents or do not report these, despite being lawfully obliged to do so by the GDPR. The ability to academically research these inside incidents becomes more difficult because of this, and grasping the full extent of the impact of malicious and accidental insider incidents also becomes harder.

Over the years, more attention has come towards the insider threat, and the human factor in general is being taken more seriously nowadays, as in concurrence by the interviews. The cyber advisory field recognises the importance of the study of human culture and behaviour within organizations, but according to the interviews, organizations themselves do not always

fully understand the importance of the insider threat, or are choosing to ignore this factor for whatever reason, ranging from interest to insufficient funds. This is because there are tension fields rising in the field that come down to the problem of business versus security. The insider threat can manifest itself more easily if this business versus security problem is not appropriately handled within an organization. The interviews explain this by looking at how a disproportionate focus on either business or security can in its own way cause problems: too few rules leads to leniency for example while too many rules can lead to an aversion for the safety culture. Eventually, organizations should think about applying safety nets that counter both the rising insider threat, as well as external threats, with the work environment in mind. As derived from the interviews, a corporate culture that enables a safety culture and keeps everyone aboard, conscious, and aware, is a solid way to handle this problem. According to the interviews, this safety culture has to be supported by strategic management and imbed itself within the core of an organization to be effective.

Comment [SW2]: interessant

It is therefore that I conclude that overall, the extent of academic insight on insider threat knowledge in the field, is poorly and should be improved. The academic insights considering the insider threat appear to be substantially present within the leading cyber security advisory organizations in the Netherlands, but the insights appear to be lacking severely in the organizations that approach (or are approached by) the cyber advisory field. More quantitative future research is required to be able to make a generalized statement concerning the overall status of the extent of academic insights in the total field, but generalizing from this qualitative study I conclude that on a general level only few organizations outside of the cyber advisory field itself are aware of the academic insights considering the insider threat.

5.2 Extent of General Deterrence Theory representation in the field

Considering the extent of the application of GDT within the field, the interviews indicate that general deterrent techniques are indeed being applied relatively well in the field. However, it should be noted that according to the same interviews, many organizations fail to apply basic deterrent controls, or only resort to them after an incident.

When looking at the factors of people, processes, and technology, the interviews indicate that the cyber advisory field considers general deterrence techniques at all levels, which indicates that there is no longer an overreliance of focus on technology. It should be noted however that the interviews also show that most organizations in the Netherlands do have trouble recognising the importance of all levels, with the side note that this does not mean an exclusive focus on only one factor. On the factor of people, the interviews concur with the literature review that security awareness is a valuable general deterrent, non-technical solution. The interviews add that a security culture that is broadly supported by the organization is one of the best general deterrent solutions, as security becomes a core part of the business through this approach. At the technological factor, basic technological security controls, such as anti-virus, encryption, password protection etc., are absolutely mandatory according to the interviews, but they depend on the context and scope of an organization to determine how effective they are. At the process factor, the interviews indicate that general cyber deterrence is about preventive measures, mapping risks, and identifying critical systems

within an organization, where a basic structure determines responsibilities and the organization of incident response. This resembles general risk management.

Overall, this risk management approach towards cyber security is what determines the amount of GDT application per organization. The interviews indicate that attention has to be divided between general and specific cyber defence. This is complicated by the fact that general deterrence is not static as risks and threats shift and change, and cyber defence should match this accordingly. General deterrence should not be too reactive in its nature, according to the interviews, but many organizations are still incident driven by a risk – rule – reflex. This is, according to the interviews, because many organizations have not reached a level of maturity yet where they have their risk appetite in order. Vulnerabilities always lurk and identifying weak links must be paired with investments to lower chances and impact of these threats. Organizations that do not have their risk management in order, will not be able to accurately configure their general defences as they have no view on how to organise these. This is a problem of decision making and it is tied towards the ease through which security measures can be measured in their respective area. This, according to the interviews, comes down to technological factors being easy to measure and therefore easy to decide upon, while the human factor is hard to measure and therefore hard to decide upon. The interviews also indicate that often technological factors are easy to patch, while cultural and behavioural 'patches' take far more time.

General deterrence theory occupies itself with the deterrence, prevention, detection, and mitigation of cyber incidents. In the field, it is often presented in the form of a security action cycle. The interviews indicate that if deterrence or prevention somehow fail, detection and remedies have to be up to par in order to properly contain cyber incidents. It is even mentioned in the interviews that in the contemporary field, detection and mitigation should perhaps be prioritized over prevention as it is highly probable an organization gets hacked, and it is therefore crucial to have detection to make sure the hack does not remain undetected. The interviews indicate that many organizations do in fact have GDT or some deterrent aspects within their policies, but often times there is a mismatch when looking at the primary objective of the business and the security measures taken in place to enable the business to perform their duties. The security practices that are considered can be derived from frameworks that suggest best practices, such as ISO's, but almost always require a tighter fit depending on the context of the organisation, which is something that is hard to do if your risk management is not up to par.

The empirical evidence thus leads me to conclude that GDT is overall to a certain extent present in the cyber security field. Despite many organizations not having their risk assessments up to par, these organizations do partake in certain aspects of GDT within their policy. The cyber advisory field is well up to date on academic insights, but the organizations that seek their help or are being contacted by them appear to struggle in some or multiple aspects of GDT.

5.3 Extent of Social Bond Theory representation in the field

Application of Social Bond Theory insights appears to have found its way within the field, according to the interviews, but representation of the full extent of the theory remains to be questionable. One of the core principles of SBT: the natural tendency of people towards crime and social bonds supressing this crime, was not recognized by the interviews.

It was mentioned however, that organizations can have a 5% employee base that always screw up no matter what, but this does not have to be a natural inclination towards deviant behaviour. It is possible that there is a natural inclination, but according to the interviews it is far more likely that this behaviour is related towards group conformism, environmental nature – nurture, or people choosing the path of least resistance. This is an interesting take, as it would thus appear that social bonds can also strengthen an inclination towards deviant behaviour, which refutes the theory's initial proposition that strong social bonds supress a natural inclination towards crime. What we can learn from this, is that social bonds are thus effective in encouraging deviant behaviour from a standardized norm.

Another core part of SBT theory is the application of informal controls to reduce computer abuse. The interviews indicate that there is room for development in this area, and a certain carry over already exists. Organizations that feature this aspect of SBT theory usually have a certain corporate culture in mind and describe how people should interact with each other, for example through a code of conduct. Informal controls are seen by the interviews as a base of a workable work environment, and their contribution towards a healthy work culture are valuable towards managers who aim to steer their organization's culture. In this case, informal controls could be formalized, which the interviews indicate as something that should occur within (larger) organizations that require culture steering. The interviews also indicate however, that formalization of informal controls is always optional, and informal steering can take many forms that do not necessarily require formalization in order to be successful or effective. What the interviews do indicate however, is that organizations will require some part of an informal culture that fits in the broadly supported corporate security culture as this is an effective means towards security compliant behaviour.

A final aspect of SBT theory is the influence of attitude towards non conform security behaviour. The interviews indicate that policy compliance is important, but this is an ambiguous concept. At one hand, policies are in place to ensure compliance with security measures in order to reduce threats. On the other hand, too much steering can lead towards 'checkbox exercise', where measures are followed through for compliance sake, and actually do not facilitate business and lead to non-effective security. The interviews therefore indicate that it is important to understand what kind of culture roams at a certain organization and see how this culture influences certain behaviour. It is, according to the interviews, only in rare cases that this cultural and behavioural analysis actually happens.

It is therefore that I conclude that while SBT factors are regarded by the interviews as some of the most important aspects of cyber security, its application in the field is only present in a lesser extent. While the cyber security advisory sector seems to be relatively well up to date on SBT insights and apply these towards other organizations, the rest of the field appears to be lacking behind, despite showing signs of SBT application. The reason for this

appears to be, derived from the interviews, that most organizations while featuring SBT insights to some extent, rarely follow through on assessing the impact of these measures, if they are aware of them at all. A code of conduct is often (not even always) present, but feedback on how this impacts corporate culture and knowledge how to steer this process are not always present. 'Toxic', or 'diseased' corporate cultures based on fear are an example of this and the interviews also indicate that an informal basis of control for behaviour often exists, but this does not imply that this basis is used for compliance, and there have even been examples mentioned where these bonds were used to actually influence behaviour towards non-security compliant.

5.4 Extent of Social Learning Theory representation in the field

Social Learning Theory features the one of the least recognized extent of application in the field by the interviews. Most indicate that they do not recognize application of learning, copying or imitating deviant behaviour, especially during policy formation. On the other hand, during previous behavioural theories it has been stated by the same interviews how the social environment, and therefore corporate culture, is recognized as an important factor in determining behaviour.

Despite some SLT constructs not being instantly recognized by the interviews, the interviewees did indicate in their results that they saw how different aspects of the theory do appear within the field. It was recognized by the interviews that it is natural to copy behaviour from colleagues, thus a code of conduct to determine (least) expected behaviour is important. As concluded in 5.3 on SBT however, we have seen that actually few organizations in the field occupy themselves with these levels of culture and behavioural steering. The 'tone at the top' is mentioned here again, as a security culture should be broadly supported by the entire organization, with management perpetuating the desired behaviour being of great importance. The interviews do indicate however, that many organizations do not feature this kind of behaviour from upper management, and therefore struggle with significant cultural behaviour change throughout their organization. It would thus appear, that the understanding of how wishful behaviour has to be managed and facilitated has not seeped through in a lot of organizations.

The other constructs of SLT: differential association and differential reinforcement, on the basis of the interviews, are to a certain extent present in the field. In both formal and informal matters, it is indicated by the interviews that the exposure towards normative definitions favouring or appalling behaviour, as well as the expected and/or realized result from deviant behaviour play a part. In 5.2 on GDT, we have seen how on a general level deviant behaviour is discouraged through deterrent techniques. As for the exposure towards favoured or appalled behaviour, the interviews indicate that even though learning, copying, and imitation of behaviour are often not present in contemporary policies, the notion of corporate culture being essential in combatting cyber security issues resonates throughout the results. Exposure to sources of learning are seen as ways through which SLT insights can manifest themselves within organizations, but again, as indicated by the interviews, very few research is actually done on this subject and very few organizations occupy themselves with these constructs.

It is therefore that I conclude that SLT applications are out there in the field, to a certain extent, but lesser than the other theories. Even the cyber security advisory field appeared to have difficulty in fully recognizing the full extent of SLT, despite being able to actually name possible implementations of SLT constructs. What is clear however, is that only few organizations actually occupy themselves with these insights, and therefore the extent to which SLT manifests itself in the field should be categorized as lesser.

5.5 Extent of the Theory of Planned Behaviour representation in the field

Much like SLT, the extent of the TPB representation in the field is ambiguous, with the interviews indicating a difficulty in measuring, assessing, and gaining insight in the relevant data. The problem lies in organizations not knowing how to measure the influence of intention of behaviour, or refusing to share relevant data, if there even is any data in existence as the interviews indicate doubt whether or not organizations know how to deal with TPB. Despite this, the cyber advisory field easily recognizes TPB constructs, and the interviews indicate that TPB interest is indeed rising in both interest and development, albeit only by a few parties as the concept is considered fairly new in the field.

One component of TPB is attitude: the degree to which a person has a favourable or unfavourable evaluation of the behaviour in question. Social demands and social norms can influence the intention of behaviour, as well as perceived social pressure. We have previously seen during insider threat theory, SBT, and SLT, how these influencing factors are present in the field and how they are addressed at large by the cyber advisory field, and to a lesser extent by other organizations.

Another component of TPB is perceived behavioural control, or sense of self – efficacy. The interviews indicate that in the field it is difficult to prove whether something was intentional or not, and how this holds up towards the perceived self-control over the behaviour. The interviews do indicate that incidents can still happen, even with a good intention behind them. This accidental insider threat can thus spring from good intentions, and thus intention in itself is not a sole risk towards organizations. The interviews mention how intention often also requires opportunity in order to manifest to deviant behaviour, and how on a general deterrence level organizations should (but often enough do not) try to influence the amount of undesired opportunity.

Intention is the main component of TPB. The interviews indicate that stimulation of the correct behaviour, and in general more security awareness, can act as a counter towards intentional security incidents as it improves the attitude towards secure behaviour. The same goes for accidental incidents, as an approachable security culture is seen by the interviews as a better base for secure behaviour than a diseased corporate culture of fear. Though the interviews indicate that effectively removing deviant intention could prove to be difficult, they do indicate how social demand, social norm, and in general keeping up ‘the conversation’ with people could prove to counteract deviant intentions and influence attitude and therefore behaviour. The interviews mention how studies can help an organization to keep an eye out for people rapidly losing dedication. We can see here thus that if social bonds weaken, intention can shift to malicious behaviour.

Therefore, I conclude that TPB application in the field occurs only to a lesser extent, but in comparison to the other theories, more than SLT. The interviews indicate that TPB within the cyber advisory field is a well-known behavioural theory with practical applications in the field. The interviews also indicate however that in the field very few organizations understand how to apply these insights without the advisory firms stepping in. On top of this, there is a recurring problem of measurement as intention is hard to measure, as well as a problem of implementation as intention is hard to influence as well. That being said, TPB is gaining traction in the field, according to the interviews, and the extent to which academic insights are being applied in the field is rising.

5.6 Extent of Situational Crime Prevention theory representation in the field

In the field, SCP application, according to the interviews, occurs to reasonable extent within organization's policies. As SCP revolves around opportunity and motive to explain deviant behaviour, crime is seen as an ecological occurrence motivated by opportunistic factors. The interviews indicated a recognition of these opportunistic factors and how these are sought to be influenced.

Provoking or inhibiting conditions towards security behaviour are seen by the interviews as important aspects, and were mentioned to should be taken into account within cyber security policies. The interviews indicate that organizations can form these policies by using risk assessments to see which appropriate measures should be taken to reduce opportunity, depending on the context and scope per organization. It was indicated by the interviews that in trying to reduce opportunity, it is important that the general cyber security policy is in order, with the most important assets prioritized, and within the organization roles and responsibilities should be properly established. The interviews indicated that it is important that accountability and responsibilities are well established within an organisation and that responsibilities match perceived risk accordingly, but in practice many organizations fail to do this.

These conditions in the previous paragraph are facilitated, according to SCP, by certain opportunistic factors. These factors involve increasing potential effort and risk, reducing reward, lowering provocation and rendering excuses invalid. Not all interviewees recognized all opportunistic factors, with the side not that these are perhaps hard to find within a tight policy, though all interviewees recognized at least some application within their own organization, and in the field. Interestingly, these factors show crossover towards other behavioural theories, such as general opportunistic reduction through increasing risk and effort with GDT, and having a code of conduct available to lower provocation or at least make problems more approachable, sharing affinity with SBT, SLT, and TPB.

It is therefore that I conclude that SCP has found its way relatively well within the field. The interviews indicate that most opportunistic factors are in some way present, within the field, and within their own organization. Though some factors were not immediately identified, the core of SCP: reduction of opportunity, appear to be a relatively well known criminological theory that has found its way within the cyber security field, and not just cyber security advisory. Though many organizations probably do not use SCP aspects and/or a

combination of SCP with other behavioural theories to their full knowledge, the notion that opportunity reduction leads to less threat and/or risk appears to be well known, though not always used to full extent.

5.7 Final conclusion

Having concluded all of the behavioural theories, we can now answer the research question: through a multi-disciplinary approach comprised of information system security theory and criminology models, to what extent are contemporary scientific insights regarding cyber security with a focus on the insider threat applied in organization's policies? It would appear that within the cyber security advisory field, the insights of criminology models and their respective application within IS theory are represented and applied to a good extent. However, organizations that use the services of these advisory organizations, or are approached by these advisory organizations: a generalizable rest of the field, appears to be applying these scientific insights relatively poorly. The explanation for this, is that despite the relative long history of these criminology models existing, most organizations do not occupy themselves with these insights, and therefore are not able to apply these insights towards their own organization. Considering the human factor, with the insider threat specifically, it would appear that a traditional overreliance on other factors such as technology and external threats has left its mark within the field. According to the interviews, it would thus appear that most organizations are either not mature enough to occupy themselves with these scientific insights, are not aware of these insights, or choose to ignore them for various reasons. This is despite the fact that organizations would benefit greatly from these insights and be able to better defend against modern day cyber incidents, threats, and risk.

Comment [SW3]: Dit is niet helemaal duidelijk: zijn de cyber advisory bedrijven op de hoogte? Of hun klanten? Zie volgend comment

Comment [SW4]:

Comment [SW5]: Maar is die dreiging dan wel zo groot?

5.8 Recommendations

In chapter 4.7 we have seen how respondents believed improvements in the field could be made in their respective fields. Their answers varied to a certain extent, cut a common theme was found: the field lacks an interdisciplinary or 'holistic' approach. Despite the increasing knowledge of the importance of the human factor, many organizations refuse for different reasons to let go of traditional cyber security practices. When looking at the factors of people, processes, and technology, many organizations still focus on technology, despite contemporary cyber threats emerging from especially the human factor as well. The organizations that do understand this, often have trouble bringing all of these insights together, and remain stuck in a traditional way of cyber security. This is attempted to counter through 'business and IT alignment', yet culture and behaviour appear to still be underrepresented when bringing about knowledge of cyber security measures within organizations. Often times, risk management is thus not executed properly, and goals, risks, responsibility and knowledge do not align. It is therefore recommended, through the insights of this thesis, that organizations dare to let go of a lacking traditional way of cyber security, and adopt a more holistic approach that enables cultural, behavioural and criminological perspectives next to technological and organizational measures to keep their cyber security up to date in the contemporary threat landscape.

Comment [SW6]: Dit is te algemeen.

As indicated within my methodology, and in accordance with the interviews, I also recommend further research into the extent of scientific insights and their occurrence in the field. It has been indicated by the interviews that gathering the relevant data proves to be hard, therefore more attempts at both quantitative and qualitative research should be made to explore why so many organizations struggle in the contemporary cyber threat landscape and understand why so few academic insights are applied in the field.

Bibliography

Sources

Abomhara, M., Koien, G., *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,* in Journal of Cyber Security and Mobility, 4(1), (2015)

Ada, S., *Theories Used in Information Security Research: Survey and Agenda,* in Handbook of Research on Social and Organizational Liabilities in Information Security (New York 2009)

Agnew, R., *Testing the leading crime theories: an alternative strategy focusing on motivational process,* in Journal of Research in Crime and Delinquency, 32(4), (1995)

Ajzen, I., *Attitudes, Personality and Behavior* (New York 2005)

Ajzen, I., *Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior,* in Journal of Applied Social Psychology, 32(4), (2002)

Akers, R. L., *Criminological Theories: Introduction and Evaluation* (Los Angeles 1994)

Akers, R. L., *Deviant Behavior: A Social Learning Approach* (California 1985)

Albanese, J. S., *Intellectual Property and White-collar Crime: Report of Issues, Trends, and Problems for Future Research,* in Albanese, J. S., (ed.), *Intellectual Property Theft and Fraud: Combating Piracy* (New York 2007)

Albrechtsen, E., Hovden, J., *Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study,* in Computers & Security, 29, (2010)

Alhogail, A., *Design and validation of information security culture framework,* in Computers in Human Behavior, 49, (2015)

Alter, S., *a general, but readily adaptable model of information system risk,* in Communications of the Association for Information Systems, 14, (2004)

Anderson, C. L., Smith, R. H., *Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions,* in Management Information Systems Quarterly, 34(3), (2010)

Anderson, J. M., *Why we need a new definition of information security,* in Computers & Security, 22(4), (2003)

Appari, A., Johnson, M. E., *Information security and privacy in healthcare: current state of research,* in International Journal of Internet and Enterprise Management, 6(4), (2010)

Armitage, C. J., Conner, M., *Efficacy of the theory of planned behavior: A meta-analytic review,* in British Journal of Social Psychology, 40, (2001)

Bandura, A., *Health promotion from the perspective of social cognitive theory,* in Psychology and Health, 13, (1998)

Bandura, A., *Social cognitive theory of self – regulation,* in Organizational Behavior and Human Decision Processes, 50, (1991)

Baracaldo, N., Joshi, J., *A trust-and-risk aware RBAC framework: tackling insider threat,* in SACMAT'12 Proceedings of the 17th ACM symposium on Access Control Models and Technologies (Newark 2012)

Baracaldo, N., Joshi, J., *An adaptive risk management and access control framework to mitigate insider threats,* in Computers & Security, 39, (2013)

Barrett Jr., E. L., *Book reviews,* in Southern California Law Review, 44(2), (1971)

Beccaria, C., *On crime and punishments* (Indianapolis 1963)

Beebe, N. L., Rao, V. S., *Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process,* in Communications of the Association for Information Systems, 26(17), (2010)

Beebe, N. L., Rao, V. S., *Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security*, in Proceedings of the 2005 SoftWars Conference, Las Vegas, NV, (December 2005)

Breitel. C. D., *Reviews,* in The University of Chicago Law Review 37, (1970)

Bulgurcu, B., Cavusoglu, H., Benbasat, I., *Information Security Policy Compliance: An Empirical Study of Rationality – Based Beliefs and Information Security Awareness,* in MIS Quarterly, 34(3), (2010), 523 – 544

Burgess, R. L., Akers, R. L., *A Differential Association-Reinforcement Theory of Criminal Behavior,* in Social Problems, 14(2), (1966)

Caldwell, T., *Ethical hackers: putting on the white hat,* in Network Security 7 (2011)

Caputo, D. D., Pfleeger, S. L., Sasse, M. A., Ammann, P., Offutt, J., Deng, L., *Barriers to Usable Security? Three Organizational Case Studies,* in IEEE Security & Privacy, 14(5), (2016)

Chacko, A., *Cybersecurity – Integrating People, Process and Technology,* in IASA 87th annual educational conference & business show (2015)

Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q., *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,* in Computers & Security, 39, (2013)

Choo, K. K. R., Bishop, M., Glisson, W., Nance, K., *Internet – and cloud – of – things cybersecurity research challenges and advances,* in Computers & Security, 74, (2018)

Clarke, R. V. G., *Situational Crime Prevention: Theory and Practice,* in the British Journal of Criminology, 20(2), (1980)

Clarke, R. V., Felson, M., (eds.), *routine activity and rational choice, advances in criminological theory volume 5* (New Jersey 2008)

Clarke, R. V., *Opportunity makes the thief. Really? And so what?,* in Crime Science, 1(3), (2012)

Clarke, R. V., *Situational crime prevention: theory and practice,* in British Journal of Criminology, 20, (1980)

Clarke, R. V., *Theoretical Background to Crime Prevention through Environmental Design (CPTED) and Situational Prevention,* in Paper presented at the Designing Out Crime: CPTED convened by the AIC and NRMA Insurance, Hilton Hotel (Sydney 1989)

Clarke, R. V., Weisburd, D., *Diffiusion of crime control benefits: observations on the reverse of displacement* (New Jersey)

Cohen, L. E., Felson, M., *Social change and crime rate trends: a routine activity approach,* in American Sociological Review, 44, (1979)

Colwill, C., *Human factors in information security: The insider threat – Who can you trust these days?,* in Information Security Technical Report 14 (2009)

Cone, B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D., *A video game for cyber security training and awareness,* in Computers & Security, 26(1), (2007)

Cornish, D. B., Clarke, R. V., *Understanding crime displacement: an application of rational choice theory*, in Criminology, 25(4), (1987)

Cornish, D., Clarke, R., *Introduction*, in Cornish, D. B., Clarke, R. V., (eds.), The Reasoning Criminal (New Jersey 2014)

Covington, M. J., Carskadden, R., *Threat implications of the Internet of Things,* IEEE, Cyber Conflict (CyCon), (2013), accessed on http://ieeexplore.ieee.org/abstract/document/6568380/

Cressey, D. R., *The Theory of Differential Association: an Introduction,* in Social Problems, 8(1), (1960)

Cronan, T., Foltz, C., Jones, T., *Piracy, computer crime, and IS misuse at the university,* in Communications of the ACM, 49(6), (2006)

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., Baskerville, R., *Future directions for behavioral information security research,*in Computers & Security 32, (2013)

D'Arcy, J., Hovav, A., Galletta, D., *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,* in Information Systems Research, 20(1), (2009)

D'Arcy, J., Hovav, A., Galleta, D., *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,* in Information Systems Research (2008)

Davies, H., J., *The Intelligence Cycle is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine,* (2013) accessed on https://bura.brunel.ac.uk/bitstream/2438/11901/3/Fulltext.pdf

Davis, F. D., *User acceptance of information technology: system characteristics, user perceptions and behavioral impacts,* in International Journal of Man-Machine studies, 38(3), (1993)

Dhillon, G., Backhouse, J., *Current directions in IS security research: towards socio-organisational perspectives,* in Information Systems Journal, 11, (2001)

Dhillon, G., Backhouse, J., *Information system security management in the new millennium,* in Communications of the ACM, 43(7), (2000)

Eck, J. E., *Preventing Crime at Places,* in Sherman, L., Gottfredson, D., Mackenzie, D., Eck, J., Reuter, P., Bushway S., (eds.), *Preventing Crime: What Works, What Doesn't, What's Promising* (Washington 1998)

Eck, J., Weisburd, D. L., *Crime Places in Crime Theory,* in Crime and Place: Crime Prevention Studies, 4, (2015)

Eloff, M., M., von Solms, S., H., *Information security management: a hierarchical framework for various approaches,* in Computer and Security, 19(3), (2000)

Eminagaoglu, M., Uçar, E., Eren, S., *The positive outcomes of information security awareness training in companies,* in Information Security Technical Report, 14, (2009)

Felson, M., Clarke, R. V., *Opportunity Makes the Thief Practical theory for crime prevention,* in Police Research Series Paper 98 (London 1998)

Freilich, J. D., Newman, G. R., *Situational Crime Prevention,* in Oxford Research Encyclopedia of Criminology (Oxford 2018)

Fulk, J., Steinfield, C. W., Schmitz, J., Power, J. G., *A Social Information Processing Model of Media Use in Organizations,* in Communication Research, 14(5), (1987)

Glisson, W. B., Choo, K. K. R., *Introduction to the Minitrack on Cyber – of – Things: Cyber Crimes, Cyber Security and Cyber Forensics,* in Proceedings of the 561st Hawaii International Conference on System Sciences (2018)

Gonzalez, J. J., Sawicka, A. A., *framework for human factors in information security,* in Paper presented at the World Scientific and Engineering Academy and Society (WSEAS), Rio de Janeiro, (2002)

Gray, P., King, W., McLean, E., Watson, H., (eds.), Hoffer, J. A., Straub, D. W., *The 9 to 5 Underground: Are You Policing Computer Crimes?,* in Management of Information Systems (1994)

Greitzer, F. L., Hohimer, R. E., *Modeling Human Behavior to Anticipate Insider Attacks,* in Journal of Strategic Security, 4(2), (2011)

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., Hohimer, R. E., *Identifying at-risk employees: modelling psychological precursors of potential insider threats,* in proceedings of 45th Hawaii International Conference on System Sciences (Maui 2012)

Guerra, P., *How Economics and Information Security Affects Cyber Crime and What It Means in the Context of a Global Recession,* in BlackHat 2009 Turbo Talk Whitepaper (2009)

Gunter W. D., Higgins, G. E., Gealt, R. E., *Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents,* in International Journal of Cyber Criminology, 4(1-2), (2010)

Hadlington, L., *The "Human Factor" in Cybersecurity: Exploring the Accidental Insider,* in McAlaney, J., Frumkin, L. A., Benson, V., *Psychological and Behavioral Examinations in Cyber Security* (2018)

Hair, J. F., Anderson, R. E., Thatham, R. L., Black, W. C., *Multivariate data analysis* (New York 1998)

Herath, T., Rao, H. R., *Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness,* in Decision Support Systems, 47(2), (2009)

Higgins, G. E., *Gender Differences in Software Piracy: the Mediating Roles of Self-control Theory and Social Learning Theory,* in Journal of Economic Crime Management, 4(1), (2006)

Hinde, S., *The law, cybercrime, risk assessment and cyber protection,* in Computers & Security (2003)

Hinduja, S., Kooi, B., *Curtailing cyber and information security vulnerabilities through situational crime prevention,* in Security Journal, 26(4), (2013)

Hirschi, T., *Causes of Delinquency* (Berkeley 1969)

Hoffer, J. A., Straub, D. W., *The 9 to 5 Underground: Are You Policing Computer Crimes?,* in Sloan Management Review, 30(4), (1989)

Holdershaw, J., Gendall, P., *Understanding and predicting human behaviour,* in ANZCA08 Conference, Power and Place, Wellington, (July 2008)

Hollinger, R. C., *Crime by computer: correlates of software piracy and unauthorized account access,* in Security Journal, 2(1), (1992)

Holt, T. J., Burruss, G. W., Bossler, A. M., *Social learning and cyber deviance: examining the importance of a full social learning model in the virtual world,* in Journal of Crime & Justice, 33(2), (2010)

Holt, T. J., Burruss, G. W., Bossler, A. M., *Social learning and cyber deviance: examining the importance of a full social learning model in the virtual world,* in Journal of Crime & Justice, 33(2), (2010)

Huerga, F., *The Economic Behavior of Human Beings: The Instutitionalist/Post-Keynesian Model,* in Journal of Economic Issues, 42(3), (2008)

Hulnick, A., S., *What's wrong with the Intelligence Cycle,* in Intelligence and National Security, 21(6), (2006)

Humphreys, E., *Information security management standards: Compliance, governance and risk management,* in Information Security Technical Report, 13, (2008)

Hunter, R., R.C. Jeffrey, R. C., *preventing convenience store robbery through environmental design,* in R. Clarke (ed.), Situational Crime Prevention: successful case studies (New York 1997)

Ifinedo, P.,, *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,* in Information & Management, 51, (2014)

Jiang, S., Lambert, E., Jenkins, M., *East meets West: Chinese and U.S. college students' views on formal and informal crime control,* in International Journal of Offender Therapy and Comparative Criminology, 54(2), (2010)

Johnson, L., K., *Making the intelligence "cycle" work,* in International Journal of Intelligence and Counter Intelligence, 1(4), (1986)

Julisch, K., *Understanding and overcoming cyber security anti-patterns*, in Computer Networks, 57, (2013)

Kadam, A. W., *Information Security Policy Development and Implementation*, in Information System Security, 16(5), (2007)

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., *An Insider Threat Prediction Model,* in Katsikas, S., Lopez, J., Soriano, M., (eds.), Trust, Privacy and Security in Digital Business (Berlin 2010)

Karjalainen, M., Siponen, M., *Towards a meta-theory for designing information systems security training approaches,* in Journal of the Association for Information Systems, 12(8), (2011)

Katsikas, S. K., *Health care management and information systems security: awareness, training or education?* In International Journal of Medical Informatics, 60, (2000)

Kavanagh, J., *Security special report: the internal threat,* in Computer Weekly (2006)

Kim, H. G., *Development of the Dynamic Optimal Control Model for Information Security Strategy Choice to Maximize Information Security Compliance Intention,* in Korean Review of Corporation Management, 9(1), (2018)

Kraemer, S., Carayon, P., Clem, J., *Human and organizational factors in computer and information security: Pathways to vulnerabilities,* in Computers & Security (2009)

Kraemer, S., Carayon, P., *Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists,* in Applied Ergonomics, 38(2), (2007)

Krohn, M. D., Skinner, W. F., Massey, J. L., Akers, R. L., *Social learning theory and adolescent cigarette smoking: a longitudinal study,* in Social Problems, 32(5), (1985)

Kuhalampi, M., *impact of deterrence theory methods on employees'' information security behavior* (Jyväskylä 2017)

Kumar, N., Mohan, K., Holowczak, R., *Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls,* in Decision Support Systems 46, (2008)

Lakhani, K. R., Wolf, R. G., *Why Hackers Do What They Do: Understanding Motivation Effort in Free/Open Source Software Projects,* in MIT Sloan School of Management Working Paper 4425-03 (2003)

Layton, T. P., *Analysis of ISO/IEC 17799:2005 (27002) Controls,* in Layton, T. P., *Information Security Design, Implementation, Measurement, and Compliance* (2007)

Leach, J., *Improving user security behaviour,* in Computers and Security, 22(8), (2003)

Lee, J., Lee, Y., *A holistic model of computer abuse within organizations,* in Information Management & Computer Security, 10(2), (2002)

Lee, M., Lee, S. G., Yoo, S., *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004)

Lee, S. M., Lee, G., Yoo, S., *An integrative model of computer abuse based on social control and general deterrence theories,* in Information & Management, 41, (2004)

Leeson, P. T., Coyne, C. J., *The Economics of Computer Hacking*, in Journal of Law, Economics & Policy (2005)

Legg, P., Moffat, N., Nurse, J. R. C., Happa, J., Agrafiotis, I., Goldsmith, M., Creese, S., *Towards a conceptual model and reasoning structure for insider threat detection,* in Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(4), (2013)

Leonard, L., Cronan, T., *Attitude toward ethical behavior in computer use: a shifting model,* in Industrial Management + Data Systems, 105(9), (2005)

Leung, L., *Validity, reliability, and generalizability in qualitative research,* in Journal of Family Medicine and Primary Care, 4(3), (2015)

Liu, D., Wang, X. F., Camp, J., *Game-theoretic modelling and analysis of insider threats,* in International Journal of Critical Infrastructure Protection, 1, (2008)

Lundgren, B., Möller, N., *Defining Information Security,* in Science and Engineering Ethics (2017)

Madden, T. J., Scholder, P., Ajzen, E. I., *A comparison of the Theory of Planned Behavior and the Theory of Reasoned Action,* in Personality and Social Psychology Bulletin, 18(1), (1992)

Magklaras, G. B., Furnell, S. M., *Insider Threat Prediction Tool: Evaluating the probability of IT misuse,* in Computers & Security, 21(1), (2002)

Maimon, D., Malaya, O. B., Cathey, R., Hinton, S., *Re-thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors for Predicting Cyber Attacks,* in 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), (6-10 November 2017)

Mayhew, P., Clarke, R. V. G., Sturman, A., Hough, J. M., *Crime as Opportunity,* in Home Office Research Study no. 34 (London 1976)

Mayron, L. M., Hausawi, Y., Bahr, G. S., *Secure, Usable Biometric Authentication Systems,* in Stephanidis, C., Antona, M., (eds.), Universal Access in Human-Computer Interaction. Design

Methods, Tools, and Interaction Techniques for Inclusion. UAHCI 2013. Lecture Notes in Computer Science, 8009, (Berlin 2013)

McAfee, *Virtual Criminology report* (2008) accessed on https://resources2.secureforms.mcafee.com/LP=2980

Merhi, M. I., Ahluwalia, P., *Information Security Policies Compliance: The Role of Organizational Punishment,* in Proceedings of the 19th Americas Conference on Information Systems, Chicago, Illinois, (15 – 17 August 2013)

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G., *The Human Factor of Information Security: Unintentional Damage Perspective,* in Procedia - Social and Behavioural Sciences, 147, (2014)

Milhausen, R. R., Reece, M., Perera, B., *A theory – based approach to understanding sexual behaviour at Mardi Grass,* in the Journal of Sex Research, 43, (2006)

Miró, F., *Routine Activity Theory,* in J. M. Miller (ed.), The Encyclopedia of Theoretical Criminology (New Jersey)

Mohamed, A., *CW security trends for 2009,* in Computer Weekly (2009)

Moody, G. D., Siponen, M., *Using the theory of interpersonal behaviour to explain non-work related personal use of the Internat at work,* in Information & Management, 50, (2013)

Morgan, J., *Board and management responsibilities for information security,* in CIO Information Technology Governance, February 9, (2018)

Morris, N., Hawkins, G., *The Honest Politician's Guide to Crime Control* (Chicago 1970)

Moskowitz, S. L., *Cybercrime and Business: Strategies for Global Corporate Security* (Cambridge 2017)

Nakao, K., *Proactive cyber security response by utilizing passive monitoring technologies,* in IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, (2018)

Neuman, W. L., *Social Research Methods: Qualitative and Quantitative Approaches* (Essex 2014)

NIAC, *HMG IA standard No. 1, technical risk assessment part 1,* Issue 3.2 (October 2008)

Nisson, C., Earl, A., *The Theories of Reasoned Action and Planned Behavior: Examining the Reasoned Action Approach to Prediction and Change of Health Behaviors,* in Sweeny, K., Robbins, M., (eds.), *The Wiley Encyclopedia of Health Psychology* (2017)

Norman, A. T., *Computer Hacking Beginners Guide: How to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack* (ACM Digital Library 2018)

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., Whitty, M., *Understanding Insider Threat: A Framework for Characterising Attacks,* in 2014 IEEE Security and Privacy Workshops (San Jose 2014)

Odemis, M.,, Yucel, C., Koltuksuz, A., *Suggesting a Honeypot Design to Capture Hacker Psychology, Personaility and Sophistication,* in ICCWS 2018 13th International Conference on Cyber Warfare and Security (2018)

Omari, A. A., Walters, J., Deokar, A., Aleassa, H., Gayar, O. E., *Information Security Policy Compliance: An Empirical Study of Ethical Ideology,* in 46th Hawaii International Conference on System Sciences, (2016)

Orshesky, C., *Beyond technology – The human factor in business systems,* in Journal of Business Strategy, 24(4), (2003)

Padayachee, K., *An assessment of opportunity – reducing techniques in information security: An insider threat perspective,* in Decision Support Systems, 92, (2016)

Parker, D., B., *Fighting computer crime: a new framework for protecting information* (New York 1998)

Parsons, K., McCormac, A., Butavicius, M., Ferguson, L., *Human Factors and Information Security: Individual Culture and Security Environment,* in Command, Control, Communications and Intelligence Division DSTO-TR-2484 (2010)

Pattabiraman, A., Srinivasan, S., Swaminathan, K., Gupta, M., *Fortifying Corporate Human Wall: A Literature Review of Security Awareness and Training,* in Gupta, M., Sharman, R., Walp, J., Mulgund, P., (eds.), *Information Technology Risk Management and Compliance in Modern Organizations* (2017)

Peace, A., Galleta, D., Thong, J., *Software piracy in the workplace: A model and empirical test,* in Journal of Management Information Systems, 20(1), (2003)

Pieters, W., *The (Social) Construction of Information Security* in The Information Society, 27 (2001)

Ptacek, T. H., Newsham, T. N., *Insertion, Evasion and Denial of Service Eluding Network Intrustion Detection*, in Technical Report Secure Networks Inc., 1998)

Radzinowicz, L., King, J., *The Growth of Crime* (London 1977)

Randazzo, M. R., Keeney, M., Kowalski, E., *Insider Thread Study: Illicit Cyber Activity in the Banking and Finance Sector,* in NTACUSSS, *Networked Systems Survivability* (Carnegie Mellon 2005)

Rezaee, Z., Sharbatoghlie, A., Elam, R., McMickle, P. L., *Continuous Auditing: Building Automated Auditing Capability,* in Chan, D. Y., Chiu, V., Vasarhely, M. A., (eds.), *Continuous Auditing theory and application* (2018)

Rezgui, Y., Marks, A., *Information security awareness in higher education: An exploratory study,* in Computers & Security, 27, (2008)

Rhodes, K., *Operations security awareness: the mind has no firewall,* in Computer Security Journal, 18(3), (2001)

Richardson, R., North, M., *Ransomware: Evolution, Mitigation and Prevention,* in International Management Review, 13(1), (2017)

Rivis, A., Sheeran, P., *Descriptive norms as an additional predictor in the theory of planned behaviour: a meta-analysis,* in Current Psychology, 22(3), (2003)

Robinson, J., *Triandis' theory of interpersonal behaviour in understanding software piracy behaviour in the South African context,* Doctoral dissertation (February 2010)

Rosenstock, I. M., *Why people use health services,* in Milbank Memorial Fund Quarterly, 44, (1966)

Safa, N. S., Maple, C.,, Watson, T., Solms, R. V., *Motivation and opportunity based model to reduce information security insider threats in organisations,* in Journal of Information Security and Applications, 1(11), (2017)

Safa, N. S., Solms, R. V., Furnell, S., *Information security policy compliance model in organizations,* in Computers & Security, 56, (2016)

Sarch, A., *Wilful ignorance in law and morality,* in Philosophy Compass, 13, (2018)

Sarkar, K. R., *Assessing insider threats to information security using technical, behavioural and organisational measures,* in Information Security Technical Report, 15, (2010)

Sarver Jr, V. T.,. *Ajzen and Fishbein's "Theory of Reasoned Action": A Critical Assessment,* in Journal for the Theory of Social Behaviour, 13(2), (1983)

Sasse, M. A., Brostoff, S., Weirich, D., *Transforming the weakest link – a human/computer interaction approach to usable and effective security,* in BT Technology Journal, 19(3), (2004)

Sasse, M. A., Lawrence, D., Kemp, L. C., Ashdenden, D., Fléchais, I., Kearney, P., *Human vulnerabilities in security systems,* in human factors working group white paper KTN, accessed on: https://pdfs.semanticscholar.org/38b4/36a07f78056a82df1e9228b87ca145f09f9c.pdf

Savvas, A., *Big increase in cybercrime, and recession will make it worse,* in Computer Weekly (2008)

Schultz, E. E., *A framework for understanding and predicting insider attacks,* in Paper to be presented at Compsec 2002, London 30 October (2002)

Schultz, E., *The human factor in security,* in Computers & Security 24 (2005)

Shaw, R. S., Chen, C. C., Harris, A. L., Huang, H. J., *the impact of information richness on information security awareness training effectiveness,* in Computers & Education, 52, (2009)

Siponen, M., Mahmood, M. A., Pahnila, S., *Employees' adherence to information security policies: An exploratory field study,* in Information & Management, 51, (2014)

Siponen, M., Pahnila, S., Mahmood, M. A., *Compliance with Information Security Policies: An Empirical Investigation,* in Computer, 43(2), (2010)

Skinner, W. F., Fream, A. M., *A Social Learning Theory Analysis of Computer Crime Among College Students,* in Journal of Research in Crime and Delinquency, 34(4), (1997)

Smith, D., A., Garton, P., R., *Specifying specific deterrence,* in American Sociological Review, 54, (1989)

Stavrou, V., Kandias, M., Karoulas, G., Gritzalis, D., *Business Process Modeling for Insider Threat Monitoring and Handling,* in Eckert, C., Katsikas, S. K., Pernul, G., (eds.), Trust, Privacy, and Security in Digital Business (Cham 2014)

Stewart, J., M., *Cybersecurity Frameworks to Consider for Organization-wide Integration,* in Expert Reference Series of White Papers (2016)

Stones, E. K., *Mobile Communications: M – Crime and Security,* in Ph.D in Security and Crime Science, University College London Department of Security and Crime Science (June 2017)

Straub, D. W., *Effective IS Security: An Empirical Study,* in Information Systems Research, 1(3), (1990)

Straub, D. W., Nance, W. D., *Discovering and Disciplining Computer Abuse in Organizations: A Field Study,* in Management Information Systems Quarterly, 14(1), (1990)

Straub, D. W., Welke, R. J., *Coping with Systems Risk: security planning models for management decision making,* in MIS Quarterly, 22(4), (1998)

Suh, B., Han, I., *The IS risk analysis based on a business model,* in Information & Management, 41, (2003)

Sutherland, E. H., Cressey, D. R., *A Theory of Differential Association,* in Cullen, F. T., Agnew, R., (eds.), *Criminological Theory: Past to Present* (Los Angeles 2006)

Sutherland, E. H., *Principles of criminology* (Chicago 1947)

Swanborn, P. G., *Case Study Research What, Why and How?* (London 2010)

Szor P.,, *The Art of Computer Virus Research and Defense,* in Addison – Wesley Professional (2005)

Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E., *The insider threat to information systems and the effectiveness of ISO17799,* in Computers & Security 24, (2005)

Thomas, G., Low, G., Burmeister, O., *"Who Was That Masked Man?": System Penetrations – Friend or Foe?*, in Cyber Weaponry (2018)

Thompson, K., van Niekerk, J., *Combating information security apathy by encouraging prosocial organisational behaviour,* in Information Management & Computer Security, 20(1), (2012)

Tittle, C. R., Burke, M. J., Jackson, E. F., *Modeling Sutherland's theory of differential association: toward an empirical clarification,* in Social Forces, 65, (1986)

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., Lepri, B., *The Privacy Implications of Cyber Security Systems: A Technological Survey,* in ACM Computing Surveys, 51(2), (2018)

Triandis, H. C., *Interpersonal behaviour* (California 1977)

Tsohou, A., Kokolakis, S., Karyda, M., Kiountouzis, E., *Investigating Information Security Awareness: Research and Practice Gaps,* in Information Security Journal: A global Perspective, 17 (2008)

Vance, A., Siponen, M., Pahnila, S., *Motivating IS security compliance: insights from habit and protection motivation theory,* in Information & Management, 49(3), (2012)

Veiga, A. D., Eloff, J. H. P., *A framework and assessment instrument for information culture,* in Computers & Security, 29(2), (2010)

Venkatesh, V., Brown, S. A., *A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges,* in Management Information Systems Quarterly, (2001)

Voiskounsky, A. E., Smyslova, O. V., *Flow-Based Model of Computer Hackers'Motivation*, in CyberPsychology & Behaviour, 6(2), (2003)

von Solm, S. H., *Information Security Governance – Compliance management vs operational management,* in Computers & Security 24, (2005)

von Solms, R., van Niekerk, J., *From information security to cyber security,* in Computers & Security, 38, (2013)

Walker, T., *Practical management of malicious insider threat – an enterprise CSIRT perspective,* in Information Security Technical Report, 13, (2008)

Waller, I., *Preventing property crime in communities, by communities,* in Smarter Crime Control, a Guide to a Safer Future for Citizens, Communities, and Politicians (Plymouth 2014)

Werlinger, R., Hawkey, K., Beznosov, K., *An integrated view of human, organizational, and technological challenges of IT security management,* in Information Management & Computer Security, 17(1), (2009)

Wiant, T. L., *Information security policy's impact on reporting security incidents,* in Computers & Security 24, (2005)

Wikström, H., *Routine Activity Theories,* in Oxford Bibliographies Online, (2016) accessed on http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0010.xml

Williams, P. A. H., *In a 'trusting' environment, everyone is responsible for information security,* in Information Security Technical Report, 13, (2008)

Willison, R., Siponen, M., *Overcoming the insider: reducing employee computer crime through Situational Crime Prevention*, in communications of the ACM, 52(9), (2009)

Willison, R., *Understanding the offender/environment dynamic for computer crimes: assessing the feasibility of applying criminological theory to the IS security context,* in Proceedings of the 37th Hawaii international conference on system sciences (2004)

Willison, R., Warkentin, M., *The Expanded Security Action Cycle: A Temporal Analysis "Left of Bang",* in The Dewald Roode Information Security Workshop (Boston 2010)

Wortley, R., *Situational Crime Prevention and Prison Control: Lessons for Each Other,* in Smith, M. J., Cornish, D. B., (eds.), *Theory for Practice in Situational Crime Prevention* (St. Louis 2003)

Yoo, C. W., Sanders, G. L., Cerveny, R. P., *Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance,* in Decision Support Systems, 108, (2018)

Zhai, Q., Lindorff, M., Cooper, B., *Workplace guanxi: its dispositional antecedents and mediating role in the affectivity – job satisfaction relationship*, in Journal of Business Ethics, 117(3), (2013)

Websites

http://blogs.worldbank.org/edutech/worst-practice

http://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003

http://map.norsecorp.com/#/

http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

http://people.carleton.edu/~carrolla/index.html

http://people.carleton.edu/~carrolla/story.html

http://people.umass.edu/aizen/bb.html

http://searchsecurity.techtarget.com/definition/spear-phishing

http://trainingtoday.blr.com/article/most-effective-training-techniques/

http://www.cres.gr/behave/pdf/Triandis_theory.pdf

http://www.cres.gr/behave/pdf/Triandis_theory.pdf

http://www.energi.com/news/2017/01/2017-cyber-risks-to-intensify-as-hackers-become-more-cunning-report/

http://www.ignite.com.au/cyber-security-framework.html

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

http://www.sng.za.com/advisory/integrated-technology-and-governance-solutions/information-communication-and-technology-advisory/information-technology-security-solutions

https://cybermap.kaspersky.com/

https://cyberpolicy.com/cybersecurity-education/what-type-of-organizations-do-hackers-target-the-most

https://computerworld.nl/security/100431-social-engineering-praktijkvoorbeelden-en-tips

https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

https://www.ipexpoeurope.com/2018-Seminars/Cyber-Security-Keynote/Thursday-04-October-2018/Real-cases-of-social-engineering-hackers-competitors-and-insiders

https://digitalguardian.com/blog/what-cyber-security

https://docs.google.com/spreadsheets/d/1Je-YUdnhjQJO_13r8iTeRxpU2pBKuV6RVRHoYCgiMfg/edit#gid=1

https://insights.sei.cmu.edu/insider-threat/2015/07/handling-threats-from-disgruntled-employees.html

https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

https://intelligentid.com/75-insider-threats-accidental/

https://newsroom.accenture.com/news/new-report-finds-insider-corporate-data-theft-and-malware-infections-among-biggest-threat-to-digital-business-in-2016.htm

https://online.maryville.edu/blog/how-to-keep-up-with-constantly-changing-cybersecurity-threats/

https://patents.google.com/patent/US9930062B1/en

https://scramsoft.com/revenge-hacking-is-the-new-black-in-the-cybercrime-underworld/

https://searchsecurity.techtarget.com/definition/cybersecurity

https://searchsecurity.techtarget.com/definition/insider-threat

https://searchsecurity.techtarget.com/definition/information-security-infosec

https://securityintelligence.com/how-effective-is-security-awareness-training-for-threat-prevention/

https://securityintelligence.com/ignorance-is-no-excuse-but-it-is-reality/

https://security-system.insuranceciooutlook.com/cxoinsights/people-processes-and-technology-mantra-for-cybersecurity-nid-190.html

https://sucuri.net/security-reports/brute-force/?clickid=Vl-x9vx3XX6ZUlIw7M1E0zU3Ukj28VQyly8C3E0

https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/

https://threatconnect.com/blog/how-to-explain-what-is-a-cyber-threat/

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

https://www.acronis.com/en-us/articles/gandcrab/

https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp

https://www.cio.com/article/3136159/security/how-to-prevent-ceo-fraud.html

https://www.cnbc.com/2017/08/05/watch-this-russian-hacker-break-into-our-computer.html

https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

https://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html

https://www.csoonline.com/article/3267988/hacking/what-hackers-do-their-motivations-and-their-malware.html

https://www.dearbytes.com/alerts/wannacry/

https://www.enterprise-cio.com/news/2016/jan/22/importance-security-awareness-training-enterprise-it-governance/

https://www.fireeye.com/cyber-map/threat-map.html

https://www.forbes.com/sites/danwoods/2013/03/11/why-security-without-usability-leads-to-failure/#1c32b7244533

https://www.helpnetsecurity.com/2018/05/15/insider-threat-blind-spot/

https://www.iasplus.com/en/binary/dttpubs/2009securitysurvey.pdf

https://www.infosecurity-magazine.com/opinions/accidental-insiders-serious-threat/

https://www.iso.org/standard/54533.html

https://www.itgovernance.co.uk/blog/organisations-failed-by-lack-of-cyber-security-processes/

https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/

https://www.nist.gov/cyberframework

https://www.nrc.nl/nieuws/2017/06/27/volg-hier-de-ontwikkelingen-rond-de-wereldwijde-randsomware-aanval-a1564740

https://www.nytimes.com/news-event/russian-election-hacking

https://www.observeit.com/blog/new-ponemon-institute-study-insider-threats-lead-to-big-losses-and-significant-costs/

https://www.pchulplijn.nl/helpdesk/virus-verwijderen/politievirus/persoonlijke-computer-wordt-geblokkeerd

https://www.ponemon.org/blog/tag/cost%20of%20insider%20threats

https://www.pri.org/stories/2016-07-13/center-most-spy-scandals-you-can-usually-find-one-these-four-factors

https://www.pri.org/stories/2017-12-14/russia-s-influence-middle-east-growing

https://www.quora.com/What-is-the-purpose-of-computer-viruses

https://www.quora.com/Whom-do-hackers-usually-target-and-why

https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1

https://www.sagedatasecurity.com/blog/cybersecurity-roles-and-responsibilities-for-the-board-of-directors

https://www.technibble.com/why-do-people-create-computer-viruses/

https://www.techopedia.com/definition/10282/information-security-is

https://www.trendmicro.com/en_us/security-intelligence/breaking-news.html

https://www.us-cert.gov/ncas/alerts/TA16-091A

https://www.wordfence.com/

Attachment 1. Original interview sheet used for the interviews

De aannames van de theorieën zijn dat theorie uit de criminologie wereld een positief effect heeft op IS security. Deze vragen zijn bedoelt om deze aanname te toetsen en te achterhalen waar huidige IS security beleid op is gebaseerd, met een speciale focus op, maar niet exclusief, insider threat.

Insider threat
Volgens de theorie en kijkend naar de grootste (en de meest kostige) incidenten is het gevaar van de eigen medewerkers van het bedrijf die cyber schade toe richten groten dan de dreiging van buitenaf.
Q: Kijkend naar dreigingen die de mogelijkheid hebben veel schade aan te richten, zijn interne of externe dreigingen het belangrijkste focus gebied volgens u en waarom?
Q: Qua interne dreiging, hoe ziet u de verhoudingen tussen accidentiele (accidential) en opzettelijke (malicious) incidenten en hoe word hier met het opstellen van beleid rekening mee gehouden?
Q: Hoe ziet u het verband tussen een werkbare werkomgeving en een veilige werkomgeving?

GDT (General Deterrence Theory)
Volgens de theorie is crimineel gedrag logischerwijs te verklaren aan de hand van het maximaliseren van voordelen en het minimaliseren van nadelen. Insiders binnen een organisatie kunnen handelen vanuit dit principe en slaan mogelijk toe wanneer zei bevinden dat een actie hen veel voordelen brengt.
Steekwoorden:

- Afweer
- Preventie
- Detectie
- Remedie
- Formele controle

Q: Als we kijken naar het maximaliseren van voordelen en het minimaliseren van nadelen voor potentiele cyber crime, waar kan dan volgens u op algemeen gebied rekening mee gehouden worden?
Q: Beleid groeit vaak vanuit specifieke gebeurtenissen. Wat is volgens u een effectieve verdeling van aandacht op het gebied van algemene en specifieke cyber afweer?
Q: Adviseert u een cyber beleid aan de hand van een bepaalde standaard, of past u liever 'custom made' tactieken toe?

SBT (Social Bond Theory)
De theorie luidt dat zwakke sociale verhoudingen / banden aanleiding kunnen geven tot crimineel gedrag. De insider binnen een organisatie kan door weinig affiniteit met de zaak of een gebrek aan loyaliteit besluiten toe te slaan.
Steekwoorden:

- Gehechtheid
- Inzet
- Betrokkenheid
- Persoonlijke normen
- Informele / sociale controle

Q: Gelooft u dat werknemers een natuurlijke drang hebben naar crimineel gedrag die onderdrukt moet worden op een bepaalde manier?
Q: Ziet u toepassing van, of een rol voor, informele controle (oftewel sociale banden, sociale controle) binnen een cyber security beleid?
Q: Hoe ziet u de mogelijkheid tot het beïnvloeden van de houding van werknemers tegenover niet-conform security gedrag?

SLT (Social Learning Theory)
Volgens deze theorie is crimineel gedrag aangeleerd of afgekeken. De insider kan beïnvloed worden door gedrag dat hij afkijkt van anderen, of gedrag dat door zijn collega's van hem verwacht wordt maar niet conform het security beleid is.

Steekwoorden:

- Aanleren van gedrag
- Afkijken van gedrag
- Imiteren van gedrag
- Morele houding tegenover gedrag
- Sociaal milieu

Q: Word er bij het opstellen van beleid rekening gehouden met eventueel aanleren, afkijken en imiteren van 'slecht' (lees onveilig) gedrag omtrent cyber?
Q: Wat is volgens u de invloed van de bedrijfscultuur op haar werknemers en hoe belangrijk acht u die rol?

TPB (Theory of Planned Behaviour)
De theorie stelt dat intentie voorafgaat aan daadwerkelijk gedrag richting misbruik of non – conform gedrag en daardoor een belangrijke rol speelt in het verklaren van gedrag. Houding en persoonlijke gedachten over bepaald gedrag kunnen de insider zowel motiveren als demotiveren bepaald gedrag te vertonen.
Steekwoorden:

- Houding
- Normen
- Intentie
- Faciliterende condities

Q: Is er een huidige rol binnen security beleid om de intentie tot non – conform gedrag te beïnvloeden om cyber incidenten te voorkomen en hoe wordt dit aangepakt?
Q: Hoe ziet u de rol tussen intentie en het daadwerkelijk uitvoeren van gedrag bij zowel accidentiele als opzettelijke incidenten?

SCP (Theory of Situational Crime Prevention)
De theorie stelt dat criminaliteit niet alleen ontstaat wanneer er motief is, maar ook als de mogelijkheid zich hiervoor voordoet. Een insider die in eerste instantie geen plannen heeft een actie uit te voeren, kan overgehaald worden dit wel te doen als hij zich realiseert dat er een mogelijkheid voor is.
Steekwoorden:

- Moeite
- Risico
- Beloning
- Provocatie
- Excuses
- Omgevingsfactoren
- Aansprakelijkheid
- Verantwoordelijkheid

Q: Wordt er in cyber beleid rekening gehouden met condities die potentieel non security conform gedrag uit kunnen lokken ofwel kunnen hinderen?
Q: Hebben de factoren: 'moeite, risico, beloning, provocatie en excuses' huidig een rol in security beleid?
Q: Hoe word omgegaan met de factoren aansprakelijkheid en verantwoordelijkheid in een cyber security beleid?

Afsluitende vraag
Q: Naar uw mening, waar is de grootste inhaalslag op het gebied van cyber security momenteel te halen? Op welk gebied en op welke manier?

Attachment 2 Original transcription of the first interview

Interview nr. 1 - senior consultant cyber team IT advisory (non ICT and IT background)

Insider threat

Volgens de theorie en kijkend naar de grootste (en de meest kostige) incidenten is het gevaar van de eigen medewerkers van het bedrijf die cyber schade toe richten groten dan de dreiging van buitenaf.

Q: Kijkend naar dreigingen die de mogelijkheid hebben veel schade aan te richten, zijn interne of externe dreigingen het belangrijkste focus gebied volgens u en waarom?

Terecht om te stellen dat insider threat erg toeneemt. Is niet de grootste dreiging. Extern heeft een grotere dreiging. Toename in nation states landen / staten die een grotere rol spelen in het cyber crime verhaal. Veel verkeer vanuit China en Rusland. Veel gedoe met inmenging en fake news invloed uitoefenen. Meer focus op de insider threat is goed en nodig. Die insider threat is tweedelig: 1) interne medewerkers op de loonlijst zeker als multinational die met 3e en 4e partijen werken. Hier zit het toenemend gevaar. Lost raken in de mensen die in je bedrijf werken, externe bedrijven, leveranciers. Het zijn mensen die je een account geeft en toegang tot bepaalde systemen. Met veel partijen sluit je een non disclosure en geheimhoudingsverklaringen, maar dit is niet per se waterdicht en hoe manage je dat? Wie zegt dat die mensen ook handelen naar de ethiek binnen je eigen bedrijf? Moeilijk te managen.

2)

Q: Qua interne dreiging, hoe ziet u de verhoudingen tussen accidentiele (accidential) en opzettelijke (malicious) incidenten en hoe word hier met het opstellen van beleid rekening mee gehouden?

Lastige van opzettelijk is dat een bedrijf daar niet vaak uit voor wil komen. Als een bedrijf de kans heeft om het op een incident te laten lijken zullen ze dat sneller doen. Die gegevens zijn moeilijk naar boven te halen in een bedrijf, hoe vaak nu daadwerkelijk zo een data lek plaats vind. Door de AVG staat er een meldplicht vast en een termijn bijvoorbeeld na een datalek wanneer je het moet melden. Er staat alleen niet vast of het opzettelijk of een foutje moet zijn. Veel bedrijven zullen er dus niet makkelijk voor uitkomen dat er opzettelijk incidenten plaats vinden. In beleid wordt hier dus wel rekening mee gehouden: hoe ga je om met data, gegevens en wat gebeurt er als je daar op een andere manier mee omgaat.

Het is ook een juridisch stuk. Het komt neer op aansprakelijkheid. Daar zijn veel inzichten over. Wie is er voor aansprakelijk als er iets gebeurt? Er is een grijs gebied. Code of conduct, code of ethics, gedragsregels. Daar kun je mensen op aanspreken, bijvoorbeeld door een beoordelingscyclus.

Q: Hoe ziet u het verband tussen een werkbare werkomgeving en een veilige werkomgeving?

Voorbeeld: [REDACTED] de cultuur de je in een bedrijf hebt. Hoe zorg je dat veiligheid, vaak gezien als onhandig, of extra dingen, irritant, gekke dingen doen (ik wil gewoon mijn werk doen) typische spanningsvelden. Het gaat om wat voor cultuur je creëert. [REDACTED] creëert de veiligheidscultuur van het boorplatform ook in het kantoor. Niet met koffie van de trap, als je valt dan gebeurt er wat. Aanspreken wordt geduld, je mag meerderen terechtwijzen op onveiligheid. Hierdoor creëer je één veiligheidscultuur, iedereen houdt zich eraan en is daardoor erg bewust. Het kan dus heel goed samenkomen.

GDT (General Deterrence Theory)

Volgens de theorie is crimineel gedrag logischerwijs te verklaren aan de hand van het maximaliseren van voordelen en het minimaliseren van nadelen. Insiders binnen een organisatie kunnen handelen vanuit dit principe en slaan mogelijk toe wanneer zei bevinden dat een actie hen veel voordelen brengt.

Q: Als we kijken naar het maximaliseren van voordelen en het minimaliseren van nadelen voor potentiele cyber crime, waar kan dan volgens u op algemeen gebied rekening mee gehouden worden?

Het begint met preventie. Zorgen voor authorizatiebeheer, toegang tot databases afschermen, fysieke toegang moet strikt ingericht worden. Detectie, toename voor securityoperations, monitoring, detect & respond. Clientfacing en hoe ga je daar mee om. Ook hier is een tweedeling: 1) Aan de ene kant techniek: goeie tooling die precies detecteert wat je wil, tools die daar direct op in kunnen haken en jou de handvatten geven om acties uit te kunnen zetten. 2) Ook proces: zorgen ervoor dat iedereen weet wat hij moet doen. Crisismanagement, weten naar wie je moet communiceren, weten waar de verantwoordelijkheden liggen. Goeie factchecking, niet handelen op aannamen.

Q: Beleid groeit vaak vanuit specifieke gebeurtenissen. Wat is volgens u een effectieve verdeling van

aandacht op het gebied van algemene en specifieke cyber afweer?
Specifiek belangrijk zijn bijvoorbeeld zero – day vulnerabilities. Kwetsbaarheden in tooling of software die voor niemand nog bekent is. Bijvoorbeeld wannacry. Je kunt hier moeilijk op anticiperen dus daar kun je niet een eenduidig beleid op hebben. Er word zeker wel rekening mee gehouden, maar het zijn dingen die heel plots aan het licht komen. Ingrijpende zwakheden in systemen die dan ook voor hackers ineens zero – day zijn. Hackers en bedrijven racen dan als het ware met elkaar tussen uitbuiting en bescherming, dat gat moet zo snel mogelijk gedicht worden. Specifieke cyber afweer is dan dus een proces of maatregelen dat je zou moeten hebben in het geval van een zero day, hoe schaal je op en hoe verdeel je de prioriteit. Algemene cyber afweer zit hem dan meer in preventie maatregelen, zorgen dat de risico's goed in kaart zijn, duidelijkheid welke systemen bedrijf kritisch zijn. Systemen met klantgegevens onderkennen bijvoorbeeld meer risico's en daar pas je dan je beleid op aan.
Q: Adviseert u een cyber beleid aan de hand van een bepaalde standaard, of past u liever 'custom made' tactieken toe?
Dubbel. Je wil altijd een uitgangspunt nemen. Een bepaald framework kan hiervoor handvaten bieden omdat het onderwerpen betreft in een cyber keten waar je iets mee moet. Aan de andere kant is zo'n standaard nooit helemaal 100% passend en zal er altijd iets van customization aan te pas moeten komen. De kroonjuwelen van een bedrijf zijn vaak zo waardevol dat je daar extra maatregelen voor draait. Dit kan je doen aan de hand van een standaard, preventie, detectie, awareness maatregelen, maar er zal altijd customization aan toegepast moeten worden.
SBT (Social Bond Theory)
De theorie luidt dat zwakke sociale verhoudingen / banden aanleiding kunnen geven tot crimineel gedrag. De insider binnen een organisatie kan door weinig affiniteit met de zaak of een gebrek aan loyaliteit besluiten toe te slaan.
Q: Gelooft u dat werknemers een natuurlijke drang hebben naar crimineel gedrag die onderdrukt moet worden op een bepaalde manier?
Nee. Geloof er zelf niet in.
Q: Ziet u toepassing van, of een rol voor, informele controle (oftewel sociale banden, sociale controle) binnen een cyber security beleid?
Zeker. De bedrijfscultuur is hier heel belangrijk. Met elkaar afspreken en elkaar de ruimte geven om elkaar aan te spreken omtrent veiligheid. Op het gebied van cyberveiligheid zit daar zeker een rol in. Dit zit heel dicht bij security awareness. Hoe maak je mensen bewust en bekwaam in het handelen melden en herkennen van risico's. Dat is dus zeker belangrijk. Informeel, zeker op het gebied van awareness en het vergroten van de cultuur is management commitment. De top, het management, moet het duidelijk uitstralen en communiceren dat security belangrijk is. Daarmee maak je een stap in het creëren van de juiste cultuur en ik geloof er zelf in dat ondanks dat er best een hiërarchische laag kan zijn, voelt niemand dat echt zo. Geen partners hoog in de boom.
Q: Hoe ziet u de mogelijkheid tot het beïnvloeden van de houding van werknemers tegenover niet-conform security gedrag?
Dit gaat over de balans tussen ga je werken met sancties of werken met beloningen. Je kunt mensen belonen op goed gedrag, bijvoorbeeld na een phishing test beloon je ze met chocolade of een mok waar 'I'm aware' op staat. Dit droeg bij aan de motivatie en de zichtbaarheid van security. Tegelijkertijd kun je niet zonder beleid met sancties tegenover foutief handelen. Er zijn veel theorien over hoe je daar mee om moet gaan. Er zijn mensen die zeggen dat sancties averechts werken, of juist wel maar alleen op de juiste manier.
SLT (Social Learning Theory)
Volgens deze theorie is crimineel gedrag aangeleerd of afgekeken. De insider kan beïnvloed worden door gedrag dat hij afkijkt van anderen, of gedrag dat door zijn collega's van hem verwacht wordt maar niet conform het security beleid is.
Q: Word er bij het opstellen van beleid rekening gehouden met eventueel aanleren, afkijken en imiteren van 'slecht' (lees onveilig) gedrag omtrent cyber?
Ja. Wanneer collega's bepaalde dingen doen ben je snel geneigd dingen ook zo te doen. Dat is mens natuurlijk. Terugkomend op zaken als code of conduct. Er moet goed vastgelegd worden wat er van mensen verwacht wordt. De bedrijfscultuur is heel belangrijk, maar wel best lastig. Zeker grote, internationale bedrijven waar veel verschillende culturen en inzichten bij elkaar komen. Hoe kom je

tot een common handelen van mensen en inzicht van hoe je met elkaar werkt. De verschillende culturen binnen een bedrijf zouden kunnen botsen. Cultuur is iets belangrijks, maar moeilijk te veranderen, kan vaak niet 'binnen een dag'. Er word wel getracht dit voor elkaar te krijgen. Door security audits en interviews met het management en trainingen mensen bewust en klaar maken voor een security omgeving. Dit zijn ook dingen die je moet herhalen en dit zijn lastige trajecten die veel tijd kosten.
Q: Wat is volgens u de invloed van de bedrijfscultuur op haar werknemers en hoe belangrijk acht u die rol?
Heel belangrijk. (zie ook vorige vragen). Dit is een van de grootste randvoorwaardes voor veilig handelen binnen een bedrijf. Als je niet met elkaar een bepaalde overtuiging kan creëren van hoe je met zaken om moet gaan en niet mensen de ruimte geeft om daar ook inspraak op te hebben of elkaar op aan te spreken dan wordt het lastig om goede maatregelen te nemen.
TPB (Theory of Planned Behaviour)
De theorie stelt dat intentie voorafgaat aan daadwerkelijk gedrag richting misbruik of non – conform gedrag en daardoor een belangrijke rol speelt in het verklaren van gedrag. Houding en persoonlijke gedachten over bepaald gedrag kunnen de insider zowel motiveren als demotiveren bepaald gedrag te vertonen.
Q: Is er een huidige rol binnen security beleid om de intentie tot non – conform gedrag te beïnvloeden om cyber incidenten te voorkomen en hoe wordt dit aangepakt?
Iemand die al iets in zijn hoofd heeft dat hij iets uit gaat halen, hoe halen we de intentie daar weg? Valt af te vragen of je daar iets aan kunt doen. Veel bedrijven moeten een soort assessment doen waarin gevraagd word of je handelt naar de juiste maatstaven, of er zaken zijn gebeurt die eigenlijk niet kunnen. Maar die intentie, ik vraag me af of je dat makkelijk bij iemand weghaalt. Stelt vraagtekens bij hoe je daar beleid op aanpast. Belangrijk om goed met mensen te blijven praten, kijken of mensen happy zijn binnen een bedrijf. Misschien is het wel beleid, dat je een goed gevoel houdt met de werkvloer. Daarin kun je makkelijk red flags zien waar een persoon er niet echt lekker meer in zit, heeft niet meer de dedication en dan met iemand daarover in gesprek gaan.
Q: Hoe ziet u de rol tussen intentie en het daadwerkelijk uitvoeren van gedrag bij zowel accidentiele als opzettelijke incidenten?
Gedragstheorie achtige wetenschap. Ik denk dat mensen toch wel enigszins terughoudend zijn naar het handelen van hun intentie. Toch wel bij die insider, echt wel veel mensen ontevreden zijn over zaken en toch wel met de gedachten lopen wat uit te halen of wat te doen. Tegelijkertijd is het lastig om daar gegevens op te halen want veel bedrijven zouden dat niet zomaar openlijk publiceren. Grote incidenten door een insider zijn op één hand te tellen, terwijl incidenten van hackers die kun je op meerdere handen tellen. De intentie en het daadwerkelijk handelen is beperkt en de gegevens zijn ook beperkt, dus het is moeilijk om te toetsen. Ik zou insider threat definiëren als een insider met opzettelijk kwade intentie.
SCP (Theory of Situational Crime Prevention)
De theorie stelt dat criminaliteit niet alleen ontstaat wanneer er motief is, maar ook als de mogelijkheid zich hiervoor voordoet. Een insider die in eerste instantie geen plannen heeft een actie uit te voeren, kan overgehaald worden dit wel te doen als hij zich realiseert dat er een mogelijkheid voor is.
Q: Wordt er in cyber beleid rekening gehouden met condities die potentieel non security conform gedrag uit kunnen lokken ofwel kunnen hinderen?
De insider threat neemt wel toe, met name omdat er een veel diversere landschap werkt aan mensen die werken met je systemen. Dan is de vraag wat is een insider, iemand met mogelijk opzettelijke intentie, dat kan dus ook iemand zijn die een insider wordt, bijvoorbeeld een contractor, die bij een belangrijk project betrokken is of toegang heeft tot allerlei data en daar worden absoluut maatregelen op genomen. Als er een project op wordt gestart wordt voor een nieuw IT systeem er een assessment gedaan welke data wordt gebruikt in dit project en welke data wordt uiteindelijk gebruikt in het systeem en aan de hand van een vragenlijst kun je dan makkelijk bepalen welke voorwaarden gesteld moeten worden bij werken met een 3e of een 4e partij. Dat is een voorbeeld van duidelijk beleid en risk assessment waarbij maatregelen horen die worden getroffen om die opportunity zoveel mogelijk te beperken.
Q: Hebben de factoren: 'moeite, risico, beloning, provocatie en excuses' huidig een rol in security

beleid?
Moeite: Phishing is een goed voorbeeld. Binnen een dag kun je een mooie phishing mail opstellen, voor een paar dollar fix je een paar email adressen of deze lijst maak je zelf en dan ga je aan de slag. Hoe meer moeite iemand moet doen om hiermee aan de slag te gaan hoe beter dat voor de security is.
Risico: belangrijk om altijd mee te nemen in je beleid. Alles hangt vast in het traditionele enterprise risk, wat is het risico, als het risico laag is, dan is daar minder focus op. Risico voor de dader is bij cybercrime interessant. Vaak is het risico hier kleiner dan in traditionele criminaliteit. Het is heel anoniem, vaak kun je online anoniem blijven waardoor de crime erg aantrekkelijk is. In veel gevallen waar mensen wel gepakt zijn waanden ze zich risicoloos.
Beloning: werkt twee kanten op. Voor een hacker is het een van de interessante dingen, financieel gewin en reputatie. Op forums van hackers scheppen ze op tegen elkaar, in de scene willen ze laten blijken dat ze de beste zijn. Er zijn ook gevallen bij mensen die fraude hebben gepleegd, als insider, die dan toch hun mondje voorbij praten. Door dit met mensen te delen vallen ze door de mand. De andere kant op, voor het bedrijf, is dit verlies. Dit zit in een risico assessment ook, als je kijkt naar bepaalde risicos, wat is de impact en wat is het financiële loss dat je kan hebben. Als dit te hoog is ga je maatregelen treffen.
Provocatie: er zijn vaak veel goeie initiatieven om mensen die wellicht kwade intenties hebben middels beloningen juist uit te nodigen om te hacken. Sites voor ethical hackers of gewone hackers die als ze succesvol iets hacken hier geld voor krijgen. Grote partijen zoals Google of Microsoft loven dan een geld bedrag uit voor hackers, white hat maar soms ook black hat om fouten te vinden en op deze manier hun systeem sterker te maken.
Excuses: kun je niet zo makkelijk beleid op voeren. Misschien awareness, mensen op de hoogte brengen van wat het beleid is. Je ziet dat veel bedrijven een security awareness programma optuigen, dit is dan vaak e-learning, maar je ziet dan dat mensen eigenlijk toch te weinig leren. Excuses als ‘ik wist niet dat we zo handelen’ of ‘ik heb niet de kennis of kunde om IT dingen te regelen, dus mijn IT afdeling moet maar zorgen dat ik geen phishing mailtje krijg’, dat zouden eigenlijk geen excuses moeten zijn maar juist maatregelen, iemand kan je heel goed trainen, bij phishing mails, waar moet ik op letten.
Q: Hoe word omgegaan met de factoren aansprakelijkheid en verantwoordelijkheid in een cyber security beleid?
Aansprakelijkheid, verantwoordelijkheid is een juridisch vraagstuk als je het op individuele personen betrekt. Dit zit al vaak gebakken in beleid.

Afsluitende vraag

Q: Naar uw mening, waar is de grootste inhaalslag op het gebied van cyber security momenteel te halen? Op welk gebied en op welke manier?
Persoonlijk wat ik belangrijk vindt is integratie tussen alle onderdelen van het bedrijf. Je hebt generiek IT risk management, systemen optuigen en continuiteitsproblematiek. Dan heb je echt security, echt technisch de security maatregelen die je neemt. Je hebt ook je generieke risk management, die enterprise risk management, exposure, regulators, te maken met dingen als avg en gdpr, hoe komt dit nu allemaal samen? Hoe zorg je voor dat je een duidelijk beeld kan vormen over de impact, eigenlijk de rol van cyber in dat geheel. Wat ik vaak zie is ondanks veel business en IT alignment plaatsvind, dat is dat business en IT samenwerken, moet ook cyber daar ook nog steeds meer een onderdeel in worden. Ik denk dat daar nog wel een uitdaging ligt. Daarmee zeg ik niet dat veel bedrijven te weinig doen op het gebied van cyber, dat kan misschien altijd meer, heel veel bedrijven hebben vaak wel precies in zicht wat er moet gebeuren op het hoogste niveau en dat veel bedrijven ook wel goeie stappen zetten, maar om dat allemaal bij elkaar te brengen , dus dat je zorgt dat IT afdelingen, security afdelingen en ook business toch nog meer in een geheel gaan werken dat is toch best een uitdaging.

Attachment 3 Original transcription of the second interview

Interview nr. 2 – senior manager Cyber (IT Advisory) (ICT and IT background)

Insider threat

Volgens de theorie en kijkend naar de grootste (en de meest kostige) incidenten is het gevaar van de eigen medewerkers van het bedrijf die cyber schade toe richten groten dan de dreiging van buitenaf.

Q: Kijkend naar dreigingen die de mogelijkheid hebben veel schade aan te richten, zijn interne of externe dreigingen het belangrijkste focus gebied volgens u en waarom?

De perceptie is in de beleving van klanten wel dat extern de grootste dreiging is. Veel van de maatregelen, waaronder beleid, is gericht op dreigingen vanaf de buitenkant terwijl een aspect waar wij veel aandacht aan besteden in ons programma, de onderliggende cultuurdrijvers die je ook nodig hebt om de interne dreigingen zichtbaar te maken en te voorkomen dat die niet altijd even goed belicht worden. Intern is dus zeker wel belangrijk, en wat ik ervaar bij de klanten is dat daar bij de klanten vaak wat minder aandacht voor is dan de externe dreigingen.

Q: Qua interne dreiging, hoe ziet u de verhoudingen tussen accidentiele (accidential) en opzettelijke (malicious) incidenten en hoe word hier met het opstellen van beleid rekening mee gehouden?

Naast het cyber team is er ook een forensisch team dat zich meer bezig houdt met fraude. Wij zitten meer aan de kant van voorkomen en detectie en respons daarop. Je kunt beiden wel zien. Er worden wel een aantal vangnetten geregeld voor het onopzettelijk maken van fouten. Dan kunnen dat verband controles zijn of meerdere mensen die nodig zijn om toegang te krijgen tot gegevens, maar ook een aantal detectiemiddelen om in de gaten te houden of mensen geen dingen doen die niet de bedoeling zijn.

Q: Hoe ziet u het verband tussen een werkbare werkomgeving en een veilige werkomgeving?

Dat is altijd een spanningsveld. Vanuit een security team, vanuit een CISO, die wil de lat veel hoger leggen dan vanuit het business veld is gewenst of toegestaan en afhankelijk van hoe de governance binnen een organisatie is geregeld worden bepaalde maatregelen wel of niet doorgevoerd. Heel lastig om iets te implementeren dat in de praktijk niet de werkzaamheden van de business niet belemmeren.

GDT (General Deterrence Theory)

Volgens de theorie is crimineel gedrag logischerwijs te verklaren aan de hand van het maximaliseren van voordelen en het minimaliseren van nadelen. Insiders binnen een organisatie kunnen handelen vanuit dit principe en slaan mogelijk toe wanneer zei bevinden dat een actie hen veel voordelen brengt.

Q: Als we kijken naar het maximaliseren van voordelen en het minimaliseren van nadelen voor potentiele cyber crime, waar kan dan volgens u op algemeen gebied rekening mee gehouden worden?

Het is een combinatie van verschillende zaken zoals autorisatie, detectie en respons. Je kunt stellen dat voor cyber crime in het algemeen, maar ook voor interne dreiging of fraude, je kan alles inrichten maar je gaat het toch niet voorkomen als mensen de intentie hebben om fraude te plegen. Als je daar over nadenkt, zeker in een samenspel van meerdere medewerkers dan ga je dat niet voorkomen. Hetzelfde zie je met cyber incidenten, in de praktijk, ook met de inbraaktesten die we zelf doen, ergens binnen komen is niet het punt. Het punt is ongemerkt binnen komen en zorgen dat je onopgemerkt blijft totdat je hebt waar je voor komt. Dus bij veel van onze klanten zit daar de winst te behalen. Kijk je moet wel preventie hebben anders komen er honderden tegelijk binnen, maar het is een illusie om te denken dat je daarmee de problemen voorkomt. Je mag er wel vanuit gaan dat partijen binnen komen en zo niet al binnen zijn.

[Q: zou je kunnen zien op algemeen gebied dat bij detectie en remedy wat te behalen valt]

Ik denk dat je dan moet zorgen dat je detectie zo snel is dat je zo kort op het incident zit dat je daarmee de schade kan beperken en dat betekend dus ook dat de voordelen die je als fraudeur of insider daaruit kan halen daarmee worden beperkt.

Q: Beleid groeit vaak vanuit specifieke gebeurtenissen. Wat is volgens u een effectieve verdeling van aandacht op het gebied van algemene en specifieke cyber afweer?

Een methode om de aandacht te verdelen is een inschatting van kans en impact van een incident en op basis daarvan vaststellen welke maatregelen je dan meer of minder aandacht geeft. Daarmee classificeren we dan vaak het risico en als je dat in een matrix uitzet en waar dingen dan hoog uitkomen dan weet je dat je daar meer aandacht in moet steken. Je kunt dat op een x en een y asje uitzetten. Je ziet dat veel, op het gebied van technische kwetsbaarheden, daar kun je een impact rating

aan geven, daar kun je gewoon een getal aan koppelen. Voor technische maatregelen is dat makkelijke dan iets wat onder 'organisatie' of 'proces' valt, maar dan kan het nog steeds. 99% Veilig betekend 100% kwetsbaar, want als aanvaller heb je maar één deurtje nodig om binnen te komen. Dus het heeft niet zo heel veel zin om heel veel energie te steken in een aantal oplossingen, terwijl er aan de achterkant gewoon een ingang is om te gebruiken. Dus die risico verdeling en eigenlijk zoeken wat is nou de zwakste schakel in de keten en daarin juist investeren met zo'n kans en impact inschatting is heel belangrijk anders investeer je gewoon in de verkeerde dingen.
Q: Adviseert u een cyber beleid aan de hand van een bepaalde standaard, of past u liever 'custom made' tactieken toe?
Belangrijk onderscheid dat je ziet, ondanks de meerdere verschillende modellen, is dat ze compliance based zijn, of risico gebaseerd. Wat ik net omschrijf dat zit meer in een risico gebaseerde aanpak waarbij je niet probeert volgens een ISO standaard alle boxjes probeert af te checken maar ook te kijken wat is nou de effectiviteit van de maatregelen die genomen zijn. En dat kan betekenen dat je bepaalde maatregelen in de omgeving waar het over gaat of in het dreigingsbeeld voor je organisatie waar je het over hebt dat die meer focus krijgt dan anderen.
SBT (Social Bond Theory)
De theorie luidt dat zwakke sociale verhoudingen / banden aanleiding kunnen geven tot crimineel gedrag. De insider binnen een organisatie kan door weinig affiniteit met de zaak of een gebrek aan loyaliteit besluiten toe te slaan.
Q: Gelooft u dat werknemers een natuurlijke drang hebben naar crimineel gedrag die onderdrukt moet worden op een bepaalde manier?
Dat word iets te sterk gesteld. Ik geloof dat er een correlatie is tussen de veiligheidscultuur in een organisatie of waar inderdaad betrokkenheid een van de aspecten is en het uiteindelijke gedrag dat je dan in een organisatie ziet. Wat mij betreft is deze wat te negatief geformuleerd. De driehoek, motief, middel en gelegenheid die dan een situatie kan creëren waarin mensen dat gedrag kunnen vertonen ik denk dat het een minderheid is die daar een natuurlijke drang naar heeft.
Q: Ziet u toepassing van, of een rol voor, informele controle (oftewel sociale banden, sociale controle) binnen een cyber security beleid?
Dat is uiteindelijk de basis van een werkbare situatie. Of je in een omgeving werkt waar alles met harde controles en sancties moet dichttimmeren dan kom je in een vrij onwerkbare situatie terecht. Het is wel interessant want wij doen ook allerlei security awareness trainingen en je ziet dat veel organisaties dan investeren in allerlei e-learning oefeningen of workshops terwijl er soms in groepen echt iets mis is op het vlak van de cultuur of betrokkenheid. Dan heeft zo'n club net een reorganisatie achter de rug of er hangt er eentje in de lucht en ze weten niet of ze er over 3 maanden nog werken en dan ga je ze in een workshop zetten nou ja ik geloof daar niet in. Dat is totaal geen motivatie om die kennis zo tot zich te nemen of toe te passen dan kan je een hele bak kennis aanslepen, maar in mijn beleving werkt dat minimaal.
Q: Hoe ziet u de mogelijkheid tot het beïnvloeden van de houding van werknemers tegenover niet-conform security gedrag?
Daar kan je van alles mee doen, ik heb een modelletje die kan ik je even laten zien. [laat een model zien op een labtop]. Als je kijkt naar het beïnvloeden van gedrag van werknemers als het gaat om het creëren van een veiligheidscultuur dan hebben we eigenlijk 8 dimensies dit is een wetenschappelijk model dat 20 jaar geleden door een van onze partners ontwikkeld is aan de hand van een groot aantal onderzoeken en daar zit al een aantal preventieve, detectieve en respons achtige gedragsdrivers in, waar je aan kan sleutelen om uiteindelijk het gedrag van medewerkers te beïnvloeden. Dus we meten vaak, het begint vaak met questionnaires en interviews om de zelf perceptie vast te stellen: wat is nou bepaald gedrag in een organisatie. Voorbeeldgedrag is dan heel interessant, als je dat het management vraagt dan krijg je een hele andere uitslag dan als je dat op de werkvloer vraagt. Als die scores teveel afwijken van elkaar, dan heb je wel iets om over te praten. Dus hiermee kijken we dan bijvoorbeeld voor spaar een diagrammetje uit vaak [???] op basis van wat initieel onderzoek om te kijken wat zijn dan de aspecten die dan sterk of minder sterk vertegenwoordigd in een organisatie en dat geeft je dan de richting waar kun je het beste aan sleutelen. Dus dan een plaatje uit een rapport was handhaven van het beleid een duidelijk onderbelicht aspect en dan kun je daarmee wat handvaten geven om op dat vlak dingen te versterken en daarmee toch het gedrag te beïnvloeden. Dus, bij dit plaatje, we kijken naar het beïnvloeden van gedrag specifiek in relatie tot awareness, zijn dit eigenlijk de

verschillende componenten waar we dan in onze aanpak naar kijken. Aan de ene kant zijn dat meer kennis en vaardigheden dus dit zit meer aan de trainings kant dit zit meer in de kant met de oefeningen dus dan heb je het bijvoorbeeld over dat we een phishing mail met malware hoe gaan mensen daar nou mee om, klikken ze daarop of gaan ze dat melden. In de organisatie, maar ook als baas zijnde [???] middelen ter beschikking stellen om aan de cultuur wat bij te voegen.

SLT (Social Learning Theory)

Volgens deze theorie is crimineel gedrag aangeleerd of afgekeken. De insider kan beïnvloed worden door gedrag dat hij afkijkt van anderen, of gedrag dat door zijn collega's van hem verwacht wordt maar niet conform het security beleid is.

Q: Word er bij het opstellen van beleid rekening gehouden met eventueel aanleren, afkijken en imiteren van 'slecht' (lees onveilig) gedrag omtrent cyber?

Ik vraag me af of dat in die zin gebeurt. Ik denk dat het niet veel verder gaat dan wat sturen of misschien het aanspreken van je collega's. Aanspreekbaarheid hadden wij als een van de aspecten in dat plaatje zitten. Een voorbeeld dat ik heb, wat alleen niet echt in het beleid terug komt, een belangrijk element dat wij wel zien is de toon 'at the top', als het management niet het voorbeeld gedrag geeft wat ze zelf willen dat het wordt uitgevoerd, dat je daarvan direct kopieer gedrag ziet bij de rest van de werknemers. Dat is dan wel een element wat we heel sterk meenemen, of dat dan ook zodanig terugkomt in beleid, dat denk ik niet. We beginnen met dit soort trajecten wel altijd bovenaan, in de organisatie, als het daar niet lukt, hoe kun je dan verwachten dat het bij de werknemers gebeurt, als ze daar niet het voorbeeld zien, dan denken ze 'nou leuk die training pfff' maar de baas doet het ook niet dus succes ermee. Andersom gebruiken we het ook, dus in de social engineering oefeningen die we soms doen, een van de dingen die we proberen is telefonisch medewerkers te manipuleren in het vrijgeven van gevoelige informatie. Kijken of ze data willen opsturen of uploaden of weet ik veel wat onder valse voorwendselen. Een van de trucjes die we dan gebruiken is zeggen van 'we hebben al je collega's al gebeld, niemand vindt het een probleem, alleen bij jou is het een probleem', om dan in het onderbewust iets te veranderen in iemands hoofd dat hij meer geneigd is in te stemmen. In combinatie met andere psychologische trucjes is dat iets wat iemand wel over de streep kan trekken.

Q: Wat is volgens u de invloed van de bedrijfscultuur op haar werknemers en hoe belangrijk acht u die rol?

Fundamenteel. Het staat niet voor niets in het modelletje als basis.

TPB (Theory of Planned Behaviour)

De theorie stelt dat intentie voorafgaat aan daadwerkelijk gedrag richting misbruik of non – conform gedrag en daardoor een belangrijke rol speelt in het verklaren van gedrag. Houding en persoonlijke gedachten over bepaald gedrag kunnen de insider zowel motiveren als demotiveren bepaald gedrag te vertonen.

Q: Is er een huidige rol binnen security beleid om de intentie tot non – conform gedrag te beïnvloeden om cyber incidenten te voorkomen en hoe wordt dit aangepakt?

Ik zie dat niet terug in beleid, behalve dat je dan… uiteindelijk is werknemer tevredenheidsonderzoek een middel om dit soort dingen in ieder geval in kaart te brengen en dan.. ik denk dat het vaak samen gaat met ontevredenheid of te hoge werkdruk of andere aspecten waardoor de betrokkenheid is afgenomen of al beperkt was en dat dat leidt dan tot de intentie om op een andere manier misschien niet tekortkomingen te compenseren. Want als je werknemer tevredenheidsonderzoeken serieus uitvoert en opvolging aan geeft dat je voor een deel dit soort aspecten kan terugdringen. Zit dat in beleid? Nou misschien in HR beleid dat je dat daar kunt vinden.

Q: Hoe ziet u de rol tussen intentie en het daadwerkelijk uitvoeren van gedrag bij zowel accidentiele als opzettelijke incidenten?

Beiden kunnen voorkomen. In het cyberdomein denk ik dat je meer te maken hebt met incidentiele of accidentiele situaties waarin medewerkers iets gedaan hebben omdat ze gewoon niet opletten of het zo makkelijker leek, of ze eigenlijk geen kennis hebben van de mogelijke impact en gevolgen. Er zijn altijd situaties waarin intentie ook een rol speelt. Ik heb het beeld dat dat er minder zijn. Het is namelijk lastig om te meten, als je er mee weg komt, komt het niet voor in de statistiek dus is het moeilijk er iets over te zeggen. Het is vaak dat achteraf blijkt dat er middelen tegen zijn, ik denk dat een groot deel van die groep er toch mee weg komt.

SCP (Theory of Situational Crime Prevention)

De theorie stelt dat criminaliteit niet alleen ontstaat wanneer er motief is, maar ook als de mogelijkheid zich hiervoor voordoet. Een insider die in eerste instantie geen plannen heeft een actie uit te voeren, kan overgehaald worden dit wel te doen als hij zich realiseert dat er een mogelijkheid voor is.

Q: Wordt er in cyber beleid rekening gehouden met condities die potentieel non security conform gedrag uit kunnen lokken ofwel kunnen hinderen?

In de wat grotere bedrijven zie je dat heel veel, de gelegenheidsfactor zo klein mogelijk maken, of dat je autorisaties en logging van authorizaties geregeld zijn om de kans van ongewenst gedrag zo klein mogelijk te maken en als je dan iets doet dat er in ieder geval vastlegging van is en dat het beeld ervan in de log files staat. Er komen ook allerlei familiebedrijven, dat is dan op basis van vertrouwen geregeld en dat gaat dan in de praktijk mis omdat daar dan buitenstaanders bijkomen of dat een bedrijfje iets groeit en die controle is dan eigenlijk niet geregeld. Je ziet bestwel veel klanten die zijn begonnen als familie bedrijf en die hebben dan eigenlijk wel behoefte aan die maatregelen. Je zou in het beleid toch wel een aantal zaken inrichten om gelegenheid elementen terug te dringen.

Q: Hebben de factoren: 'moeite, risico, beloning, provocatie en excuses' huidig een rol in security beleid?

Moeite: in het beleid zie je wel dat er allerlei stappen genomen worden om de moeite die je als aanvaller, er van uitgaande van het perspectief van een fraudeur, om die zo groot mogelijk te maken, alsmede het risico. Een voorbeeld is het aanbrengen van een gelaagde vorm van beveiliging waar je allerlei [???] moet doorbreken om tot de systemen te komen.

Aan de beloningskant kun je daar ook dingen mee doen. We doen zaken met crypto bedrijfjes, die in de bitcoins en andere zaakjes zitten, maar een heel beperkt deel opslaan op systemen die ook intern toegankelijk zijn en dan de beloning daarvan dus tot een minimum te brengen. Die hebben er ook beleid voor om dat te optimaliseren zodat niet het grote geld ergens staat waar volgens plan iemand bij kan. Minimaliseren van de assets die echt nodig zijn en de rest wegbergen op een plaats met nog extra beveiligingsmaatregelen.

Provocatie: [laat plaatje zien]. Dit soort oefeningen, twee collega's trekken een uniform aan en gaan on geautoriseerd een bedrijf in, in opdracht van de directie, verder weet niemand dat en die proberen dan dossiers te stelen of systemen te hacken of noem maar wat en als iemand ze aanspreekt zeggen ze 'nee we zijn hier om de airco's te repareren', dus dan zoek je eigenlijk zeg maar de provocatie op, want je wil dat mensen hen aanspreken of naar buiten escorteren of de security bellen, dus eigenlijk het achterwege laten van gewenst gedrag is dan provocatie en op allerlei manieren kan je dat doen. Dit heet een social engineering assessment of een social engineering oefening. Het hangt er van af waar je op uit bent, dus als we er in zetten als een training is het een assessment, als we in kaart willen brengen wat nou daadwerkelijk een risico is, zonder dat daar voor de individuele werknemer zeg maar het oefenen en het leren daarvan op de eerste plek staat, dan noemen we dat vaak een red teaming. Dan moet je meer denken aan een soort 'Oceans 11' achtige scenario waar we proberen financiële middelen buit te maken of patiëntgegevens in handen te krijgen en dat soort zaken. Dus de leerfactor zit hem dan veel meer in de teams en het security operations center, incident response teams, management teams, rvb niveau, hoe gaan die omschakelen als ze echt een major incident hebben. Dat zijn vaak echt hit and run scenario's waar soms collega's door de politie worden afgevoerd. Dit word vaak door de staff aangevraagd die de rest van hun werknemers op deze manier wakker willen schudden. Vaak vindt hierna ook een replay fase na, waar nog een keer langs alle stappen gaan om te kijken waar het nou mis ging en wat je hier nou had moeten doen. We werken veel samen met onze forensische experts die bij echte incidenten betrokken worden en we lenen dan wat we in de praktijk zien en dat passen we toe bij onze eigen oefening zodat we zien waar ook organisaties bijblijven, wat zijn nu de trends in de onderwereld en waar houden die zich mee bezig.

Excuses: herken ik niet zo.

Q: Hoe word omgegaan met de factoren aansprakelijkheid en verantwoordelijkheid in een cyber security beleid?

Wat we wel eens tegen komen is dat verantwoordelijkheden en met name in de incident response organisatie of op management niveau dat die niet duidelijk overlegd zijn. Dat is een vraag die we wel eens stellen als we bij een bank zitten is als we nu eens te maken hebben met een cyber aanval, wie heeft dan het mandaat om op die 'knop' te drukken dat heel het internet bankieren offline gaat en dan weet je, dan sta je binnen 5 minuten op nu.nl en een uur later ben je op de NOS, wie mag er nou op

die knop drukken? Dit is vaak niet voor allerlei scenario's afgesproken, dus op het moment dat die situatie zich voordoet, dat dan de discussie moet worden gevoerd hoe dat dan gaat en of er nou opvolging op komt of niet. Dus eigenlijk het klaarleggen van allerlei scenario's, dus als 'dit of dit' zich nou voordoet, wie mag dan besluiten of wie moet dan wat besluiten, dat is een oefening die we met veel van onze klanten wel doen en dan zie je dat ze op heel veel situaties toch niet goed voorbereid zijn. Dat vastleggen van de aansprakelijkheden en verantwoordelijkheden, dat laatste misschien wat minder, dat is wel een aspect dat we dan ook meenemen.

Afsluitende vraag

Q: Naar uw mening, waar is de grootste inhaalslag op het gebied van cyber security momenteel te halen? Op welk gebied en op welke manier?

Ik denk dat je nog steeds ziet dat bij veel organisaties de menselijke factor an sich dat die een onderbelicht onderwerp is, als je kijkt naar wat er in andere maatregelen geïnvesteerd wordt. Dat komt naar mijn beeld met name omdat de verbetering daarin best lastig te meten is. Je hebt het over het algemeen dan over lange termijn veranderingen en het is heel moeilijk om in een cultuur of het [???] aspect echt meetbaar op korte termijn te scoren. Het is ook heel lastig, een server die patch je of een security appliance zet je erbij, je test het en het is klaar en een maand later moet je dan nog een update uitvoeren, maar je kan het redelijk afvinken. Je kan niet van medewerkers zeggen is hij nou veilig of niet. Je kunt hem allerlei trainingen aanbieden, of probeert een ander kunstje, de volgende keer gaat het weer mis. Juist doordat dat zo lastig te meten is, en daarmee dus ook voor bestuurders moeilijk om te zeggen 'we hebben hier zoveel in geïnvesteerd, wat hebben we dan behaald, hoeveel incidenten hebben we niet gehad?' Doordat dat op de korte termijn moeilijk vast te stellen is, denk ik dat dat toch een achterblijvend onderdeel is in je verdediging terwijl juist als je kijkt bij de trend rapporten van incidenten erbij pakt, in 8 / 10 is de menselijke factor eigenliijk de frontlinie van zo'n aanval. Ook als wij ergens proberen een foothold te krijgen op het netwerk, dan is dit de eerste verdedigingslaag waar je doorheen moet om binnen te komen. Het gebeurt zelden dat wij proberen binnen internet servers om een server te hacken of weet ik veel wat, het is vaak via de menselijke factor veel makkelijker en veel kortere route naar waar je eigenlijk naar toe wil.

Ik denk dat die factor an sich in veel gevallen te weinig aandacht aan besteed wordt en dan in het bijzonder voor risicogroepen binnen organisaties. Dus dat betekend dan mensen met directe toegang tot gevoelige gegevens, dus dat kunnen bijvoorbeeld financiële controles zijn. Mensen die ik op het target lijstje zet als we zo'n oefening doen, of die criminele organisaties op het target lijstje zetten omdat ze transacties mogen goedkeuren, die mensen zou je juist vanuit een cyber perspectief of vanuit een fraude perspectief extra moeten trainen met beleid vind ik, dat gebeurt niet overal. Ik denk dat je in veel organisaties aan de hand van het dreigingsprofiel, dus wat zijn eigenlijk de partijen die ons potentieel aanvallen en waar moeten we rekening mee houden, wat voor middelen zetten ze in en wie zullen ze dan targetten binnen onze organisatie, dan kun je redelijk snel een lijstje maken in ieder geval wie er extra getraind moeten worden. In de praktijk zie je vaak dat die gewoon mee gaan in het bredere programma dat is geregeld. Terwijl bijvoorbeeld CIO fraude dat is zo'n voorbeeld, er is een telefoontje of mailtje, die lijkt van de CIO te komen, maar het is dan eigenlijk een list om geld uit een geheim potje onbedoeld over te maken. Dus werknemers die dat soort posities hebben, die moet je extra trainen voor dit soort zaken.

Attachment 4 Original transcription of the third interview

Interview nr. 3 – Business, Security, Research & Development, Security Services Manager

Insider threat

Volgens de theorie en kijkend naar de grootste (en de meest kostige) incidenten is het gevaar van de eigen medewerkers van het bedrijf die cyber schade toe richten groten dan de dreiging van buitenaf.

Q: Kijkend naar dreigingen die de mogelijkheid hebben veel schade aan te richten, zijn interne of externe dreigingen het belangrijkste focus gebied volgens u en waarom?

Als je kijkt naar de mogelijkheid dan zijn het veel interne medewerkers of interne dreigingen de belangrijkste, maar dan kijk je naar de mogelijkheid. Als je kijkt naar wat je daadwerkelijk ziet gebeuren, dan ligt het toch andersom denk ik. In heel veel security rapportages zie je dat insider threat het grootste risico is, ofwel bedoelt of onbedoeld en dan de interne dreigingen ontevreden medewerkers, frauduleuze medewerkers, onbekwame medewerkers die hebben de potentie om grotere schade aan te richten. Aan de andere kant durf ik wel te stellen dat de meeste schade toch wel vanuit de externe kant aangericht word, externe kwaadwillende.

Q: Qua interne dreiging, hoe ziet u de verhoudingen tussen accidentiele (accidential) en opzettelijke (malicious) incidenten en hoe word hier met het opstellen van beleid rekening mee gehouden?

Wat ik net in de vorige vraag ook al aangaf, als we kijken naar insider threat dan heb je het toch vaak over medewerkers, over leveranciers, over business partners, over inhuur mensen, 3e partijen, maar het is wel goed om onderscheid te maken want enerzijds heb je eigen medewerkers, je hebt ingehuurd personeel maar [REDACTED] maakt gebruik van open en vrij werk, je ziet dat je de in de kantine gewoon binnen kunt komen ook als je de receptie gewoon voorbij loopt, dan heb je met bijvoorbeeld leveranciers of businesspartners. Die hebben ook voor een deel toegang tot [REDACTED] zelf dus tot interne faciliteiten. Als je dan kijkt naar de verhoudingen tussen ‘per ongeluk’ en ‘opzettelijke’ incidenten, dan denk ik dat als er incidenten vanuit medewerkers gepleegd worden: ‘iedereen heeft er wel eens een rotte appel tussen zitten’. Dan is dat met name accidenteel, dus onopzettelijk. Terwijl kwaadwillende toch wel bewust de grenzen opzoeken om [REDACTED] te bestoken. Wij hebben duizenden malen per dag last van DDOS aanvallen, met malware, met virussen, dat is wel echt opzettelijk en kwaadaardig.

We kunnen het wel zien als dit gebeurt door een interne bron, maar ik denk dat er al heel veel stappen gezet zijn om dat te voorkomen. Wat wij zien vanuit [REDACTED] HR beleid, het aanname beleid, zijn er een aantal stappen gezet. Enerzijds moeten medewerkers een VOG hebben, die is al nodig bij het aanname beleid, daarnaast hebben we ook een register van medewerkers die bij ons ooit ontslagen zijn wegens fraude of kwaadaardig gedrag, want je wil niet dat zo’n rotte appel bij een ander deel van de organisatie solliciteert en weer binnen komt. In die hoedanigheid vangen we een deel op met HR beleid, we doen ook altijd een referentie background check, mensen krijgen een assessment vaak, die word soms overgeslagen maar mensen krijgen wel een background check, men moet referenties aanleveren dat is wel belangrijk, zeker in de security wereld, dat is enerzijds. Anderzijds als je kijkt naar het CISO beleid, dat is er op gericht dat mensen ook echt opgeleid worden om de juiste dingen te doen. Er komt elke maand wel een toets voorbij die ik moet halen over de bedrijfscode, over integer gedrag en dat gaat heel breed dat gaat niet alleen over cyber crime of cyber security, dat gaat letterlijk over hoe ga je om met cadeautjes die je krijgt van leveranciers, hoe ga je om met pestgedrag naar je medewerkers of collega’s, wat is wel toelaatbaar en wat is niet toelaatbaar, hoe ga je om met de bescherming van de digitale middelen? Mag je zomaar alle apps downloaden? En daar wordt ook echt op getraind. Als je die toets niet haalt dan blijven ze je ook reminders sturen dat je beter je best moet doen om hem wel te halen en als je dan niet reageert dan word je manager ingelicht. Dat is dan ook iets wat we naar onze klanten toe adviseren. We hebben ‘ons [REDACTED] CISO beleid’, wij worden best wel vaak gevraagd door klanten hoe wij dat nou doen binnen [REDACTED]. We hebben dan ons [REDACTED] CISO (corporate information security officer) beleid gratis beschikbaar gesteld in de Apple Store, dat is onze interne security afdeling, die hebben een eigen beleid geschreven dat is vrij uitgebreid en dat hebben wij dus beschikbaar gesteld aan iedereen die dat wil downloaden. Open Source dus, waarom wij dat doen, men vraagt ons hoe wij dat doen en ik denk juist dat door kennis te delen in deze industrie wij elkaar kunnen versterken, want niemand is helemaal veilig.

Q: Hoe ziet u het verband tussen een werkbare werkomgeving en een veilige werkomgeving?

Die is altijd leuk, security versus usability. Ik ben van security, dus ik timmer het liefst alles helemaal dicht. Als ik 's avonds boodschappen doe bij de Albert Heijn en ik zie van dat stoom boven de groenten uitkomen dan denk ik gelijk 'hey is dat te hacken'. De gemiddelde persoon heeft dat niet ben ik achter gekomen. Een veilige werkomgeving is essentieel de werkomgeving werkbaar te houden. Alleen gebruikers willen daar geen last van hebben. Ik vraag wel eens aan onze consultants: jongens, wat is nu de grootste concern van een van onze klanten [ziekenhuis] en dan zegt iedereen: patiëntendossiers, patiënteninformatie, privacy, dan zeg ik: nee jongens, waarvoor kom je in een ziekenhuis? Mensen in een ziekenhuis willen andere mensen beter maken. Die willen de beste zorg verlenen, die willen goede basis uitvoer, die willen zorgen dat mensen weer gezond worden en naar huis gaan. Dat is wat een ziekenhuis is. En quite frankly, de gemiddelde arts in het ziekenhuis interesseert het geen reet wat er met de patiëntengegevens gebeurt zolang het maar voldoende beschermd is dat hij zijn patiënten op een goede manier kan helpen. Die denkt niet na over of zijn anti – virus nog is geüpdatet, of of de patiëntengegevens wel veilig zijn opgeslagen. Daar zit de concern niet van een arts. Ook niet van het ondersteunend of verplegend personeel en ik denk dat je daar ook rekening mee moet houden als je kijkt naar een werkbare werkomgeving en een veilige werkomgeving. Drie kwart van Nederland is niet heel erg bezig met veiligheid, die willen alleen een werkbare werkomgeving. Alleen, die werkbare werkomgeving wordt wel gefaciliteerd door de omgeving veilig te houden. Dus je moet wel degelijk wat aan je security doen, je moet alleen zorgen dat mensen er zo weinig mogelijk last van hebben, of begrijpen waarom het er is.

GDT (General Deterrence Theory)

Volgens de theorie is crimineel gedrag logischerwijs te verklaren aan de hand van het maximaliseren van voordelen en het minimaliseren van nadelen. Insiders binnen een organisatie kunnen handelen vanuit dit principe en slaan mogelijk toe wanneer zei bevinden dat een actie hen veel voordelen brengt.

Q: Als we kijken naar het maximaliseren van voordelen en het minimaliseren van nadelen voor potentiele cyber crime, waar kan dan volgens u op algemeen gebied rekening mee gehouden worden?

Een van de belangrijkste punten is het 4- ogen principe en een scheiding van functies en verantwoordelijkheden. Het is heel simpel. Degene die de inkomende facturen goedkeurt, keurt niet de betaling goed. Dat is een scheiding van functies en verantwoordelijkheden. Als je een parallel trekt naar de fysieke veiligheid, de meeste inbraken bij mensen thuis zijn gelegenheid inbraken. Dat is omdat mensen een deur open laten staan, dat is tenminste wat ik begrepen heb, een raam open laten staan, als dan een inbreker voorbij komt denkt die dat dat wel een quick win is, dus gaat hij het doen. Gelegenheid, geen planning van tevoren. [REDACTED] is in 2012 gehackt door een scholier, een gelegenheidshacker. Hij keek of het kon. Je hebt in hackersgroeperingen heel veel verschillende soorten. Enerzijds heb je concurrenten die informatie willen stelen, echt kwaadwillende die het voor het geld doen, je hebt white hat hackers die de good cause willen dienen maar je hebt ook statelijke actoren. Je hebt ook script kiddies, dat zijn die jongens die kijken of het kan. Ik denk dat het met heel veel personen nog wel is, even los van de statelijke actoren dat is een andere doelgroep dat zijn ook heel sophisticated attacks, de nations states, rusland etc. ik denk dat je rekening moet houden met een scheiding van taken en verantwoordelijkheden om op die manier de gelegenheid te ontnemen bij mensen om iets zomaar kwaadwillends te kunnen doen. Het 4 – ogen principe om de kwaliteit van je eigen dienstverlening goed te houden. En daarnaast iets wat ook in Cyber Security Build Nederland omschreven werd: basic controls. Heel veel organisaties hebben nog geen basic controls ingezet, denk aan anti virus, firewall, security beleid, echt de basics op orde hebben. Ik vergelijk het maar even zo: bij mij thuis is ingebroken en ik wist dat er bij mij in de omgeving veel werd ingebroken en ik moest nog nieuwe sloten. Mijn buren hadden dat al allemaal maar ik moest het nog doen. En wat is er nou gebeurt, is er bij mij ingebroken omdat mijn sloten nog niet op orde waren en die van mijn buren wel. De inbreker probeert het bij het ene huis, lukt niet, gaat naar het volgende huis. Ik kon mijzelf wel voor mijn kop slaan, maar dat is hetzelfde als wat er met security gebeurt. Heel veel partijen nemen eigenlijk niet de basic security measures, die implementeren ze niet, die controls nemen ze niet en dan gaat het mis, dan is er een incident en dan begrijpt iedereen dat je er wat aan moet doen. Maar het moet eerst wel zover komen.

Q: Beleid groeit vaak vanuit specifieke gebeurtenissen. Wat is volgens u een effectieve verdeling van aandacht op het gebied van algemene en specifieke cyber afweer?

It depends. Het maakt uit welk type organisatie dat je hebt. Het maakt van de risk appatite van jouw

organisatie, het maakt uit hoe jouw organisatie opgezet is. Ik kan mij voorstellen dat netbeheerders enerzijds veel investeren in security, gewoon cyber security, om stroom netwerken niet plat te laten leggen, maar anderzijds is de grootste angst misschien wel dat iemand met een tractor een stroompaal omver rijdt waardoor heel Zuid Holland zonder stroom zit. Dus je moet je niet gek laten maken op cyber security niveau. Voor een telecom maatschappij is het digitale netwerk essentieel. Dat is waar wij onze klanten mee faciliteren, daar ligt onze core. Als vandaag dit hoofdkantoor bij wijze van spreken in brand vliegt omdat iemand met een bus naar binnen rijdt met allerlei brandbare middelen, dan hebben wij over een uur, in ons uitwijk centrum, deze hele operatie up and running. Binnen een uur. Dus voor ons is fysiek wel van belang, je wil niet dat in elk pand zomaar een vrachtwagen naar binnen rijdt, maar de cyber afweer is voor ons wel echt meer van belang en dat scheelt een beetje meer per type organisatie. Je kunt niet één sticker op heel BV Nederland plakken.
Q: Adviseert u een cyber beleid aan de hand van een bepaalde standaard, of past u liever 'custom made' tactieken toe?
Wij werken op basis van standaarden, maar meerdere standaarden vervolgens verrijken wij die met de ervaring van onze teams, met de ervaring die wij opdoen als [REDACTED] zelf, want wij zijn niet alleen de security service provider naar de markt toe, wij zijn ook afnemer. We verrijken dat weer met andere best practices. Denk bijvoorbeeld aan ISACA. ISACA is een soort branchevereniging voor risk management. Die hebben bepaalde frameworks voor risk management, maar we hebben ook het CRAM framework, NIST directive, dat zijn allerlei frameworks die komen van informatie beveiliging die voor ons van belang zijn om mee te nemen, maar dat verrijken we met informatie van het Nationaal Cyber Security Centre, van de NCTV van team high tech crime. En op basis van onze eigen ervaring, van wat wij zien dat er gebeurt in de markt op basis daarvan adviseren wij onze klanten of ontwikkelen wij beleid. Je ziet ook dat beleid niet statisch is. Het staat niet nu en over een jaar staat het nog, het is heel dynamisch. Op het moment dat er grote updates zijn in de [REDACTED] security policy dan word hij ook per mail naar iedere medewerker gecommuniceerd.
SBT (Social Bond Theory)
De theorie luidt dat zwakke sociale verhoudingen / banden aanleiding kunnen geven tot crimineel gedrag. De insider binnen een organisatie kan door weinig affiniteit met de zaak of een gebrek aan loyaliteit besluiten toe te slaan.
Q: Gelooft u dat werknemers een natuurlijke drang hebben naar crimineel gedrag die onderdrukt moet worden op een bepaalde manier?
Nee absoluut niet. Wat je ziet is dat heel veel mensen juist een natuurlijke neiging hebben tot het vertrouwen van andere mensen. En als je de neiging hebt naar crimineel gedrag, zal je eerder mensen wantrouwen denk ik. Samenwerken gebeurt op basis van vertrouwen. Als je kijkt naar monteursorganisaties, tot aan de top van [REDACTED] maakt niet uit welk segment je pakt binnen [REDACTED], dan moet men op elkaar kunnen vertrouwen om samen te werken. Ook [REDACTED] kent rotte appels. We hebben een helpdesk: security & compliance daar kunnen meldingen gedaan worden door collega's op het moment dat zei denken dat er iets niet in de haak is. Collega's of wat dan ook kunnen doorgegeven worden. Stel dat ik een collega zou hebben waarvan ik denk dat die niet chic handelt. Dan zou ik daarover zijn manager in moeten lichten, hemzelf of zijn manager. Als ik daar onvoldoende vertrouwen in heb of mij niet prettig bij voel, dan kan ik ook direct naar de security compliance. Sowieso, als ik denk dat iemand niet volgens de [REDACTED] bedrijfscode heeft gehandeld, dus echt bewust niet integer heeft gehandeld ben ik verplicht dat te melden bij de security & compliance helpdesk.
[Q: adviseert u dit ook richting uw klanten, zo'n soort bedrijfscultuur?]
Nee wij kijken op dit moment niet echt naar de cultuur. We kijken echt naar het security beleid. Dan kijken wij naar People Process Technology and Governance. Dus People, hoe ga je om met de mensen. Hoe kan je hen de juiste gedragingen aanleren door hen vooral veel voorbeelden te geven van: dit is gewenst gedrag dit is ongewenst gedrag. Dan kijken we naar technology en processen, hoe kunnen wij organisaties adviseren om mee te bewegen in de digitale verandering die er aan komt, of die nu al bezig is en welke technische controles kunnen ze nemen om dat te sturen of inzichtelijk te maken om cyber incidenten te voorkomen. We kijken ook naar de governance. We hebben boardroom games om juist het bestuur van organisaties mee te nemen in de wereld van security. Vaak denkt men dan heel simplistisch: 'Oh ik doe A dus B komt', terwijl dat met security niet altijd het geval is.

Q: Ziet u toepassing van, of een rol voor, informele controle (oftewel sociale banden, sociale controle) binnen een cyber security beleid?
Wat wij doen, informeel, is dat wij guest lectures houden. GHP, gisteren was er nog eentje. Wij nodigen mensen uit het veld uit om een lezing of presentatie te geven over iets waar zei goed in zijn en daar kan iedere medewerker zich bij aan sluiten. Klanten kunnen daar ook bij aansluiten, klanten van [REDACTED] ook, juist om op die manier het evangelie te promoten, maar niet alleen vanuit [REDACTED] zelf te laten zien dat wij samen werken. Dat is een vorm, niet van informele controle, maar informele sturing. We organiseren kennis sessies, dat doen we ook op middelbare scholen bijvoorbeeld, om toch te leren wat gewenst gedrag is: 'don't flash your boobies online', 'verzamel geen dick pics', dat soort gekkigheden. Als je dan kijkt, informeel, ik val een beetje over het woord 'controle', want dat is bij ons formeel belegd.
Qua kennisdeling doen we dat wel en verder eigenlijk heel minimaal, omdat bij [REDACTED] gewoon heel veel formeel is geregeld. Echt heel veel. Dat moeten wij ook, want iedereen heeft het nu over GDPR, terwijl wij ons al jaren moeten houden aan de telecommunicatie wet en die is veel zwaarder dan de GDPR. Dus wij telecompartijen zien dat alles kapot georganiseerd is.
Ik denk dat je vooral een cultuur moet neerzetten op basis van vertrouwen. En vertrouwen betekend dat je van je medewerkers het beste probeert te maken. Dus door kennisdeling, maar dat je ook ingrijpt op momenten dat er iets mis is.
Q: Hoe ziet u de mogelijkheid tot het beïnvloeden van de houding van werknemers tegenover niet-conform security gedrag?
Dat is heel breed. Wij hebben het zelf duidelijk beschreven, hij komt voor in de KSP [REDACTED] Security Policy. Het overtreden van regels binnen [REDACTED] kan een berisping of waarschuwing of ontslag op staande voet opleveren, ligt eraan wat er aan de hand is. Ik denk dat dit essentieel is, voor iedere organisatie in Nederland, om jouw medewerkers security compliant gedrag te leren als het ware. In de wereld hebben wij te maken met vergaande digitalisering. Als we kijken naar Nederland, wij doen zaken met andere landen, daar heb je gewoon digitale technologie voor nodig. Maar ook alles wat wij wel zelf produceren in Nederland, daar zit op een of andere manier [???] technologie in verwerkt. Denk aan die melkmachines, denk aan de Heinz Ketchupfabriek of aan ASML. Technologie, aangestuurd op een of andere manier door of een embedded systeem of IT technologie of OT technologie, om de economie op die manier draaiende te houden. Er is maar bijna niks meer waar alleen mensenwerk aan te pas komt en geen geprogrammeerd iets. Om dat draaiende te houden, de hele berg aan netwerk lijnen en data en alles wat overgaat in control te houden, zal je je medewerkers security compliant gedrag moeten gaan aanleren. En best wel wat branches zijn nog niet zo ver, maar over 10 jaar denken we niet anders denk ik. Toen ik op de middelbare school zat kregen we ECDL, European Computer Driving License, dat is echt pijnlijk, dat. Leer je Word, Excell, Internetten ofzo, en Powerpoint. Maar dat was in die tijd nodig, want het was relatief nieuw. Nu, 20 jaar later, mijn dochter maakt op de basisschool PowerPoint presentaties en die doet dat beter dan ik, bij wijze van spreken. Dat is omdat de huidige jeugd anders opgroeit, en dat is ook met security denk ik.
Ik denk dat waar wij uiteindelijk met ECDL vaardigheden aangeleerd kregen, die vaardigheden nu essentieel zijn om überhaupt iets te kunnen doen in het leven, qua toekomst en baan, en dat is met security ook: waar wij nu nog allerlei zaken aan moeten leren aan ons personeel, zal het uiteindelijk randvoorwaardelijk zijn om business te blijven. Nee nee de menselijke factor blijft daarbij achter, dat is juist een probleem.
SLT (Social Learning Theory)
Volgens deze theorie is crimineel gedrag aangeleerd of afgekeken. De insider kan beïnvloed worden door gedrag dat hij afkijkt van anderen, of gedrag dat door zijn collega's van hem verwacht wordt maar niet conform het security beleid is.
Q: Word er bij het opstellen van beleid rekening gehouden met eventueel aanleren, afkijken en imiteren van 'slecht' (lees onveilig) gedrag omtrent cyber?
Nee, volgens mij niet. Er wordt wel rekening mee gehouden als dat collega's oneigenlijk gedrag vertonen je verplicht bent om daar iets mee te doen. Ofwel je collega daar op aan te spreken, ofwel te melden bij een manager, ofwel naar de security & compliance helpdesk te gaan. Aanspreken direct, via de manager, of via de security & compliance helpdesk dus in die hoedanigheid wordt er wel rekening gehouden met het kopiëren zegmaar van gedrag, of het toestaan / faciliteren van gedrag,

maar niet aanleren, afkijken of imiteren.
Wat wij wel doen, op internet publiceren wij wel geanonimiseerd casussen die behandeld zijn door de security & compliance helpdesk. Vooral ook om onze medewerkers te laten zien 'hey dit hoort niet op deze manier', en dan treden we dus zo op. Ik denk dat dat ook iets is wat veel klanten zouden moeten doen: maak medewerkers, leer ze enerzijds wat security bewustzijn is, maar maak ze anderzijds ook bewust van de impact die het heeft op het moment dat ze zich er niet aan houden. Dus stimuleer goed gedrag, dat is het eigenlijk.
Q: Wat is volgens u de invloed van de bedrijfscultuur op haar werknemers en hoe belangrijk acht u die rol?
Essentieel. In een cultuur waar geen vertrouwen is heeft men ook niet directe behoefte om coöperatief naar elkaar op te stellen en binnen de lijntjes te blijven. Prachtig voorbeeld is een energie bedrijf waar heel veel monteurs werken en die monteurs waren erg ontevreden over de leidinggevenden. Continu overwerken, verlofaanvragen werden net een paar dagen voor deze in zouden gaan goedgekeurd, gewoon echt onvoldoende / slecht management. En die monteurs hadden daar last van, die werden chagrijnig, klopte aan bij de directeur, maar er werd weinig aan gedaan dus het was een verziekte bedrijfscultuur. Op een dag kregen zij een berichtje binnen met een link. Een van die monteurs heeft mij gebeld: 'Hey [redacted] is dit misschien Malware of niet?' Dus ik kijk en bevestig dat het best Phishing kon zijn en gaf als advies er niet op te klikken. Vervolgens is dat in die monteurs app gezet met de waarschuwing 'pas op dit is phishing', waarop een andere monteur reageerde: 'mooi lekker met zijn allen op klikken dan kunnen we onze werkgever installeren met malware'. Zo ver kan zo iets gaan. Daar zijn bedrijven zich onvoldoende van bewust denk ik, hoe essentieel de cultuur is. Uiteindelijk was dit een phishing actie van het bedrijf zelf. Maar binnen de monteurs organisatie, de Whatsapp groep van de omgeving Utrecht heeft zo snel als zei konden de omgeving Amsterdam geïnformeerd en die informeerde Zwolle, zo informeerde al die monteurs elkaar binnen die verziekte werksfeer over hoe ze die werkgever konden dwarszitten. Ik denk dat daarmee wel laat zien dat de bedrijfscultuur heel belangrijk is. Dat geld ook voor allerlei andere organisaties. Dit is een voorbeeld van een monteurs organisatie bij een grote energieleverancier, maar hetzelfde is ook op scholen. Je moet uiteindelijk een cultuur hebben van elkaar vertrouwen en elkaar durven aanspreken en op die manier ook te kunnen leren van fouten en niet bewust fouten gaan maken. Als je mij niet zou durven aanspreken over dingen die ik verkeerd doe, hoe moet ik dan leren om beter te worden? Ik vond dit wel schokkend, want ik zit al 12 – 13 jaar in de security en je komt hackers tegen en je komt journalisten tegen die informatie proberen af te troggelen en je komt heel veel verschillende mensen tegen en disgruntled employees heb je ook, maar dat is dan een individu bij wijze van spreken, maar dit was echt een collectief! Die waren collectief ontevreden over hoe ze behandeld werden en dat ze dan bewust hun werkgever wel eens zouden kunnen besmetten met malware, nou mijn mond viel open. Hoe kan zoiets? Het is waanzin dat zo iets kan gebeuren.
TPB (Theory of Planned Behaviour)
De theorie stelt dat intentie voorafgaat aan daadwerkelijk gedrag richting misbruik of non – conform gedrag en daardoor een belangrijke rol speelt in het verklaren van gedrag. Houding en persoonlijke gedachten over bepaald gedrag kunnen de insider zowel motiveren als demotiveren bepaald gedrag te vertonen.
Q: Is er een huidige rol binnen security beleid om de intentie tot non – conform gedrag te beïnvloeden om cyber incidenten te voorkomen en hoe wordt dit aangepakt?
Dan verval je al vrij snel in reguliere termen als security awareness workshops. Trainingen, awareness trainingen, om op die manier in te steken op de bedrijfsnormen en waarden die gelden en hopen dat medewerkers die eigen maken. Wij hebben samen met CISCO en McCafee onder andere Cyber Central opgericht. Dit is een samenwerkingsverband om bestuurders en medewerkers meer informatie te geven over cyber security en dat in workshops rondom awareness workshops zegmaar met hen te delen. Dat is juist ook om te sturen op normen en waarden. In die hoedanigheid medewerkers te drijven tot het uit zichzelf veranderen van hun gedrag. En ook tot het inzicht laten komen dat ze iets moeten met security in hun eigen organisatie en hoe ze dat dan gaan regelen. Dus echt die normerende waarden aanpassen.
Q: Hoe ziet u de rol tussen intentie en het daadwerkelijk uitvoeren van gedrag bij zowel accidentiele als opzettelijke incidenten?
Als het opzettelijk verkeerd gedrag wordt, dan zit daar een intentie achter, die zijn onlosmakelijk met

elkaar verbonden. Als we kijken bij accidenteel, dus onopzettelijk gedrag, dan weet ik niet of er een hele sterke link is met intentie daar, ik denk het eigenlijk van niet. Onopzettelijk gedrag heeft niet een verkeerde intentie vaak. Stel je staat bij een printer, bij ons is het iets anders ingericht, maar bij heel veel organisaties gaat het zo: Truusje staat bij de printer, Clara komt eraan maar is haar pas vergeten, of je even snel een printje kan maken? Kun je me even binnen laten in het pand? Dat is niet omdat mensen de intentie hebben om iets verkeerds te doen, maar juist de intentie hebben hun collega's te helpen en daarmee overtredingen begaan. Dan kun je jezelf wel afvragen, hoe belangrijk is het dat je iemand binnen laat? Jij weet niet of dat ik nu nog in dienst ben of net ontslagen ben. Bij een van mijn vorige werkgevers hebben ze daar een mooie test mee gedaan, ze hebben gekeken of een collega mee kon lopen met iemand het pand in, wat was gecompartimenteerd door middel van toegangspasjes met verschillende autorisatie levels en die jongen was net ontslagen, tenminste ontslag genomen, die ging ergens anders werken en toen werd hem gevraagd of ze hem nog een halve dag in konden huren om als een soort mysterie guest social engineering opdracht te doen. En iedereen liet hem gewoon binnen en hij kon overal in want iedereen dacht dat hij nog in dienst was, terwijl dat niet zo was. Is dan de intentie verkeerd? Nee je vertoont onopzettelijk verkeerd gedrag, want je veroorzaakt wel een risico voor de organisatie, alleen de intentie is niet verkeerd, dus de koppeling tussen opzettelijk en intentie vind ik niet helemaal kloppen, die zie ik niet per se.
Er is hier een security incident geweest in mijn eerste paar weken. Ik kwam hier nieuw binnen en ik had geen pas nog. Vervolgens kreeg ik een nieuwe Dell of HP laptop, in de doos. Dus ik stond beneden, bij de deur, dus ik vraag: 'jongens kunnen jullie even voor mij open doen', dus ik sta daar met die labtop ingepakt in de doos, terwijl ik vertel 'ik ben een nieuwe werknemer en mijn pasje werkt nog niet'. Iedereen liet mij zo binnen, tot aan CISO office toe, die toen is ontploft. Die is de hele trace terug gegaan waar ik vandaan kwam en die is persoonlijk al die medewerkers gaan opzoeken om hen te vertellen dat het tegen de security compliance was. En ik was heel naïef. Maar fouten maken is menselijk, mensen blijven de rest van hun leven fouten maken en dat betekend niet dat ze intentioneel verkeerd gedrag vertonen. Of dat ze opzettelijk besluiten om nu iets tegen de werkgever te doen, het is de insider threat. De threat is er wel, maar dat is niet bewust. En daar, ondanks dat het niet bewust is, die splitsing moet gemaakt worden, ondanks dat het niet bewust is moeten mensen wel gestimuleerd worden om het juiste gedrag te vertonen.
SCP (Theory of Situational Crime Prevention)
De theorie stelt dat criminaliteit niet alleen ontstaat wanneer er motief is, maar ook als de mogelijkheid zich hiervoor voordoet. Een insider die in eerste instantie geen plannen heeft een actie uit te voeren, kan overgehaald worden dit wel te doen als hij zich realiseert dat er een mogelijkheid voor is.
Q: Wordt er in cyber beleid rekening gehouden met condities die potentieel non security conform gedrag uit kunnen lokken ofwel kunnen hinderen?
Wat je ziet is dat ons cyber security beleid op 4 assen: People, Processes, Technology, Governance in is geregeld. En los daarvan ook nog een aantal andere elementen: Identify, identificeren van risico's. Prevent, voorkomen van misbruik. Detect, detecteren dat als er toch iets is, wat er dan mis is. Respond & Recover. En dat begint enerzijds met het identificeren van risico's bijvoorbeeld bij HR beleid met de VOG etc. Dat is ook wat wij andere organisaties aanraden: identificeer wat je kroonjuwelen zijn. Wat zijn je belangrijkste assets in je organisatie en zorg dat je daar je beveiliging omheen bouwt. Neem preventieve maatregelen om te voorkomen dat criminelen binnen komen, zoals anti virus, een firewall. Als ze dan toch binnen zijn, zorg dat je ze dan detecteert, dus dat je op de een of andere manier iets van detectie mogelijkheid hebt met een IDS detection intrusion systeem, of met een monitor systeem, om te detecteren waar het mis gaat. Dan, respond zorg dat de processen en mensen in place zijn om dat op te volgen, om daar op te reageren en dat je ook recovery mogelijkheden hebt op het moment dat het helemaal mis is. Iets van uitwijk of back up. En daar zetten wij sinds vorig jaar in op predict: het voorspellen van risico's. Kunnen wij aan de hand van 1 + 1 = 3 zeggen dat we hier een signaal zien dat op zich niet leid tot een incident en daar zijn wij een signaal dat op zich niet leid tot een incident, maar als we die signalen allemaal met elkaar correleren zien we wel incidenten en hoe gaan we dan daar naar handelen?
Dus er zijn in het beleid zowel technisch als organisatorisch meerdere elementen om te voorkomen dat mensen non conform gedrag gaan vertonen. Ook in wat wij aanbieden richting klanten, daar is juist ons security portofolio op geënt.

Q: Hebben de factoren: ‘moeite, risico, beloning, provocatie en excuses’ huidig een rol in security beleid?
In het beleid wat zij zelf hebben en ook adviseren richting klanten is een respons & disclosure beleid. Als jij ons gehackt hebt, of je hebt een kwetsbaarheid gevonden en je hebt ons niet grootschalig schade toe gericht en ook niet expres je best gedaan om ons pijn te doen en het daarna direct aan ons meld zonder naar de media te stappen, dan hebben we de tijd om het in gezamenlijkheid op te lossen en daarna kun je naar de media, bij wijze van spreken. In een response & disclosure beleid waar je verantwoordelijkheid neemt als hacker en je meld het bij ons, dan krijg je een beloning. En dat is ook wat eigenlijk adviseren aan andere partijen: kijk naar zo’n beleid. Stel je hebt een script kiddie en die doorbreekt je beveiliging, dan wil je dat die zich meldt bij jou. Op het moment dat die hacker jouw organisatie veel pijn heeft gedaan dan moet er een strafrechtelijk traject gestart worden, maar als het eigenlijk alleen maar kijken of aantonen is dat er iets mis is, zorg ervoor dat je zo iemand beloond, want die geeft jou op dat moment de mogelijkheid om je beveiliging op te schonen. Mijn dochter zit op de middelbare school in de klas met twee jongens die continu de school hacken, script kiddies en ze zijn er ook nog eens goed in. Als je dat soort mensen door middel van een response & disclosure beleid de mogelijkheid geeft excuses te maken, dat helpt wel denk ik. Dat is wat wij zelf doen. Als je kijkt naar de factoren en hun huidige rol, nou dan beloning en excuses (verontschuldiging) via response & disclosure.
Moeite, risico & provocatie is wat lastig. Wij kijken zelf in het bedrijf wat is nou onze core. Wat zijn onze belangrijkste assets en daar hebben we de beveiliging omheen gebouwd. Dus risico is voor ons wel van belang.
[Q: en hoe zit dat voor de insider?]
Wij hebben een eigen CERT team (Computer Emergency Response Team), die houden ons bedrijf veilig. Die handelen tickets en meldingen af conform beleid om alles op te volgen wat mogelijk verdacht gedrag is. Verdacht gedrag wordt weer gesignaleerd door de tooling die wij inzetten. Maar ook bijvoorbeeld doordat medewerkers er niet samen uitkomen, ergens iets melden. Dus dat is best wel verworven in ons beleid. Een nieuw iets is dat wij in onze werkplek allerlei versleutelingen hebben op document. Vanuit beleid is dat ingezet, ik kan niet zomaar meer alles overal heen sturen. Ik moet daar moeite voor doen. En stel ik moet daar moeite voor doen als insider, dan word dat weer ergens anders gedetecteerd, omdat dat afwijkend gedrag is. Dus dat hangt heel nauw met elkaar samen.
Wij hebben in beleid een clean desk policy, juist om te voorkomen dat mensen zooi laten rondslingeren waardoor mensen toch nog even kijken. Jouw printer werkt alleen op het moment dat de laptop open staat, dus als ik iets wil printen moet ik hem meenemen opengeklapt en wel, super irritant. Als je het hebt over usability versus security. Alleen ik weet wel waarom dat is, juist om te voorkomen dat mensen op print drukken even koffie gaan halen en naar de wc gaan en op print hebben gedrukt, terwijl er wel een belangrijk printje bij de printer ligt. Dat zij hun schermen bijvoorbeeld altijd gelockt zijn, het is een utopie om te geloven dat iedere collega dat doet. Wat wij wel doen, om even terug te komen op informele controle, is als iemand zijn pasje laat liggen het pasje verstoppen, om er voor te zorgen dat hij het de volgende keer niet vergeet, of iemand zijn beeldscherm omdraaien of een hele afdeling sturen dat er taart beschikbaar is, weet je dat soort suffe kantoorgeintjes. Zo iets vergeet je nooit meer. We hadden een nieuwe medewerker, [redacted], die kwam uit Zuid Zeeland en hij werkt nog steeds bij ons. De eerste dag vergat hij zijn pas en die hadden we dus aan het plafond getapet, aan van die systeem plafonds. De volgende dag kwam hij, boos, en zei ‘dat doen jullie zeker altijd met alle nieuwelingen’, hij had het idee dat hij gepest werd als nieuweling. Toen heb ik hem apart genomen en uitgelegd dat hij niet gepest werd als nieuweling, maar omdat hij zijn pasje was vergeten. Een van onze salesmensen heeft meerdere keren zijn scherm open laten staan, met een toetsencombinatie kun je het beeldscherm ondersteboven parkeren. Hij was woest, we hadden hem al meerdere keren taart gestuurd en daarna weet je, [redacted] kwam ik pas nog tegen en de salesmanager ook, omdat ze zo woest waren, zijn ze nooit meer hun pasje vergeten of vergeten hun scherm te locken. Dat zijn dingen die klinken naar, maar het werkt wel. Het wordt niet vanuit het management gedaan, maar vanuit de medewerkers onderling, dan kan het. Vanuit het management heeft een te hiërarchische relatie voor dit soort dingen en dat kan niet zomaar.
Q: Hoe word omgegaan met de factoren aansprakelijkheid en verantwoordelijkheid in een cyber security beleid?

Iedereen is aansprakelijk voor zijn eigen data en voor de manier waarop je daar mee om gaat. Binnen ons bedrijf ben je persoonlijk als medewerker aansprakelijk en je hebt je eigen verantwoordelijkheid. En daar word je als medewerker ook op getoetst en beoordeeld. Ik denk dat dat, als we kijken naar de markt en het security beleid dat in de markt gezet wordt, dat daar ook nog wel een slag te halen is: zorgen ervoor dat de medewerkers begrijpen dat ze ergens voor aansprakelijk zijn. Want het is heel gek dat heel Nederland in beweging komt voor de AVG van 15 mei 2018, terwijl dat eigenlijk shit was die ze al veel eerder hadden moeten regelen, maar omdat het nu vanuit een wet georganiseerd wordt doen we het, maar niet omdat we voelen dat we iets hadden moeten doen. Als je kijkt hoe simpel camera's van kinderdagverblijven te hacken zijn, of camera's in systemen van welke instellingen dan ook, dan is dat vaak omdat standaard wachtwoorden niet veranderd zijn. Maar het zijn wel de kinderen van andere mensen waar naar gekeken kan worden, het is wel de data van andere mensen die voorbij komt bij andere organisaties en ik denk dat partijen zich daar onvoldoende bewust van zijn. Er zou veel meer gekeken moeten worden naar aansprakelijkheid en verantwoordelijkheid van iedere medewerker én de teams én de organisaties as a whole: de verschillende lagen van inzoomen, alleen dat dat nog onvoldoende gedaan wordt.

Afsluitende vraag

Q: Naar uw mening, waar is de grootste inhaalslag op het gebied van cyber security momenteel te halen? Op welk gebied en op welke manier?

Op twee dingen denk ik. Kom ik toch weer op dat irritante ECDL. Na ECDL konden wij allemaal iets met Word, PowerPoint, Outlook en Excel. Ik denk dat er echt structureel in het basis onderwijs en op middelbare scholen awareness workshops moeten komen of dat het onderdeel van het lesprogramma moet worden, dat mensen zich security bewust worden. Dat is één. Het tweede is voor heel veel partijen: kijk naar basic controls. Partijen zeggen dat ze geen geld hebben voor security. Basic control is een clean desk policy. Een clean desk policy kost geen geld. Het zorgt er wel voor dat je data niet zomaar rond slingert. Ik kwam bij [REDACTED] werken en ik had een laptop beveiligd, extra beveiligd gebouw, mocht mijn laptop niet alleen achterlaten dat wist ik, en toen ging ik naar huis dus ik heb mijn laptop op mijn bureau gezet, deur dicht gedaan en naar huis gegaan. De volgende ochtend kwam ik op kantoor, was mijn kamer op slot. En het duurde een kwartier voor de beste man van de beveiliging er was die die kamer kon openen en ik had mijn eerste formele waarschuwing want bij [[REDACTED]] mag je je laptop niet onbeheerd achter laten ook niet als je weg bent of op je kamer opbergt, tenzij je hem vastlegt aan een snoer, een bepaald locker ding. Waarom? Er staat vertrouwelijke data op. En ik vind het heel mooi dat ze zo'n beleid hebben. Daar zijn heel veel mensen zich niet van bewust. Een bakker met zijn nieuwsbrief heeft wel informatie en allerlei gegevens zoals geboortedatum, waar heeft hij die voor nodig? Zorg er voor dat je basic controls hebt die geen geld hoeven te kosten rondom je people, maar ook basic security controls, technische controls bijvoorbeeld, denk aan anti virus, een firewall, of een test voor je website, een vulnerability test kun je laten doen voor enkele tientjes. Dus het hoeft niet heel veel geld te kosten, alleen het zorgt er wel voor dat straks alle apparaten die wij in huis hebben geen onderdeel zijn van een bot netwerk of dat mijn gegevens niet overal te koop worden aangeboden. Dat is dus enerzijds de wereld voor de basic controls binnen de volwassen wereld en anderzijds echt het opleiden van de nieuwe generaties.

Attachment 5 Original transcription of the fourth interview

Insider threat – forensic senior manager

Volgens de theorie en kijkend naar de grootste (en de meest kostige) incidenten is het gevaar van de eigen medewerkers van het bedrijf die cyber schade toe richten groten dan de dreiging van buitenaf.

Q: Kijkend naar dreigingen die de mogelijkheid hebben veel schade aan te richten, zijn interne of externe dreigingen het belangrijkste focus gebied volgens u en waarom?

Ik denk dat je naar beiden moet kijken. Als je kijkt naar eigen medewerkers, dan heeft het wat mij betreft vooral te maken met dat die dagelijks bezig zijn met het beheer van allerlei vertrouwelijke data en assets die voor de organisatie belangrijk zijn. Dus vanuit criminologische gedachte hebben zei ook de mogelijkheid om daarmee allerlei zaken te doen en ook zaken die je als organisatie niet wil. Dat is één. Dus dat gaat meer uit van een soort van opzet. Daarnaast, kunnen medewerkers ook allerlei fouten maken. Dan komt wat mij betreft ook die verwevenheid met buiten want dat zijn wel twee verschillende dreigingen maar volgens mij hebben ze wel met elkaar te maken. Daar waar je in een organisatie mensen hebt die open staan om tegen wat dan ook iets verkeerds te doen met eigendommen van de organisaties, met informatie van de organisaties, dan is dat natuurlijk een interessante target voor dreiging van buitenaf. Hetzelfde geld voor het eerste punt wat ik aanhaalde, als mensen onbewust door een slordige manier van werken de organisatie kwetsbaar maken dan wordt dat ook weer interessant voor externe dreiging. Dus beiden.

Q: Qua interne dreiging, hoe ziet u de verhoudingen tussen accidentiele (accidential) en opzettelijke (malicious) incidenten en hoe word hier met het opstellen van beleid rekening mee gehouden?

Ik houd me heel erg bezig met cultuur en gedrag binnen organisaties. Even een zijstapje, ik heb ook criminologie gedaan en security management dus ik geloof er ook dus in juist dat ons gedrag heel erg beïnvloedbaar is door omgeving. Dus daar waar je een omgeving creëert waar mensen het belangrijk vinden om op een goede manier om te gaan met vertrouwelijke informatie daar waar héle duidelijke goede regels en procedures worden neergezet die mensen moeten helpen handvaten bieden om zaken op een goede manier te doen, daar is inherent de kans dat er iets mis gaat veel kleiner dan in organisaties waar daar al veel minder aandacht voor is. Waar management het belang, van bijvoorbeeld informatie beveiliging veel te weinig benadrukt, waar als er fouten worden gemaakt mensen zich niet durven opstellen laat staan fouten toegeven of incidenten durven te melden. Nou als je kijkt naar accidentele en opzettelijke incidenten, ik zeg altijd maar dat als je kijkt naar de populatie binnen een organisatie, grofweg 5% van de mensen daar hoef je nooit naar om te kijken, die zullen altijd op elk moment zonder dat iemand aanwezig is het goede doen, althans willen doen. 5% die zal je altijd in de gaten moeten houden. Als die ook maar enigszins de kans krijgen dan zullen zij de fout in gaan en dat kan bijvoorbeeld doordat zij een diefstal plegen of informatie delen. Maar het gaat juist om die middengroep, die 90% die zijn heel erg beïnvloedbaar door waar de kant van de organisatie heen valt. Dus als jij een cultuur hebt waar juist wordt benadrukt dat die 5% die het altijd goed dat, dat dat het gedrag is wat je wilt, dan geloof ik dat de grote meerderheid dat nooit vanuit opzet doet.

Q: Hoe ziet u het verband tussen een werkbare werkomgeving en een veilige werkomgeving?

[Tekent voor mij een diagram van de relatie tussen incidenten en regels] Even een zijstap, bij ziekenhuizen, daar is patiëntveiligheid heel belangrijk. Dat is een van de belangrijkste thema's. Daar is ook veel wetenschappelijk onderzoek naar gedaan, zien wij nou een relatie tussen het aantal incidenten dat gebeurt en het aantal regels dat wij opstellen om patiëntveiligheid te bevorderen, dus procedures etc. Dan blijkt dat de afdeling waar ze geen regels hebben ongeveer gemiddeld 12 incidenten meemaken. Dan ga je kijken naar afdelingen waar een paar regels zijn, daar is een daling in het aantal incidenten naar 9, dat is positief. Daarmee zou je de conclusie kunnen trekken dat regels en procedures die helpen met mensen in het juiste gedrag te krijgen. Maar wat blijkt, zo hebben ze ook gekeken naar afdelingen waar ze heel veel regels hadden waar ze alles dichttimmeren, dan blijkt zo dat het gemiddeld aantal incidenten toeneemt tot 23. Daar zijn redenen voor dat dat het geval is. Ten eerste, als je mensen heel veel regels geeft, dan gaan ze niet meer zelf nadenken dus je schakelt eigenlijk het menselijk vermogen om verbanden te leggen uit. Ten tweede, mensen die heel veel regels krijgen opgelegd worden daar zenuwachtig van omdat ze bang zijn om regels te overtreden, dat heet met een heel ingewikkeld woord: hypiagiofobia ; de angst om regels te overtreden, maar dan gebeurt het juist. Ten derde is er ook als je heel veel mensen heel veel regels oplegt, dan kan ook een bepaalde mate van aversie ontstaan tegen regels waardoor dat er bijna, moedwillig, overheen wordt

gestapt. Dat even over de regels en helderheid, dan moet je ook gaan nadenken in hoeverre die werkbare werkomgeving. Kijk, we weten uit allerlei onderzoeken dat je wel aan mensen kunt vragen: 'dit zijn de regels we willen dat je dat doet', maar je moet mensen ook faciliteren om dat te kunnen doen, dus je moet ze tijd geven om het uitvoeren, je moet ze de middelen en de kennis geven, zorgen dat de competenties worden ontwikkeld om datgene wat je van ze vraagt ook te kunnen uitvoeren. Wat daar heel nauw mee samenhangt, je hebt de term vast wel eens gehoord, dat is dat als je mensen bijvoorbeeld onder hele hoge tijdsdruk zet, dan gaan wij ons focussen op de dingen die we nog wel kunnen halen. Dat zit in onze natuur, dat zie je echt op allerlei terreinen terug. Als je mensen onder teveel druk zet, dan gaan we altijd de korte route kiezen.
Een mooi voorbeeld daarvan is, bij een teleologie faculteit in Amerika, daar werden studenten gevraagd om een lezing voor te bereiden over de barmhartige Samaritaan. Dat gaat over het verhaal dat het goed is als je iemand helpt. Die groep werd in tweeën gesplitst, de eerste groep die mocht al vast een lezing geven zelf, dat werd opgenomen op videoband over wat ze hadden geleerd, dat gingen ze dan doen en onderweg hadden ze iemand op die route neergelegd die dan duidelijk in nood was. Dan gingen ze kijken of die mensen die persoon dan gingen helpen. Tweede groep die was ook nog aan het voorbereiden op die video, maar dan zei de hoogleraar opeens dat hij de tijd helemaal vergeten was en dat over twee minuten hun lezing al was en dat ze als een gek naar hun pand moesten lopen, dat op 10 minuten afstand lag. Dus er was tijdsdruk. Ook daar hadden ze iemand neergelegd die hulp nodig had. Ondertussen bleek in de eerste groep dat 100% die man had geholpen. Bij die tweede groep nog maar 10%. Toen ze achteraf gingen vragen aan die personen waarom ze de hulpbehoevende persoon niet hebben geholpen, bleek dat de meerderheid die persoon niet eens had gezien. Ze waren er letterlijk over heen gelopen. Dat even als zijstapje wat er in ons gedrag gebeurt als we mensen onder teveel druk zetten. En zaken die het je dus ook in de werkomgeving onmogelijk maken. Dus je zult altijd moeten zoeken naar die gezonde balans tussen wel een aantal regels en vertrouwen. Dat is eigenlijk wat deze grafiek ook zegt dus je moet ook het vertrouwen hebben dat mensen gemotiveerd zijn om het goede te gaan doen. En dat zal je moeten ontdekken. Die 'sweet spot' zoeken we dan ook vaak bij klanten.
GDT (General Deterrence Theory)
Volgens de theorie is crimineel gedrag logischerwijs te verklaren aan de hand van het maximaliseren van voordelen en het minimaliseren van nadelen. Insiders binnen een organisatie kunnen handelen vanuit dit principe en slaan mogelijk toe wanneer zei bevinden dat een actie hen veel voordelen brengt.
Q: Als we kijken naar het maximaliseren van voordelen en het minimaliseren van nadelen voor potentiele cyber crime, waar kan dan volgens u op algemeen gebied rekening mee gehouden worden?
Je moet eerst weten wat voor voordelen er zijn, die zijn voor elk mens anders. De meest voordehandliggende is winst, dus geldelijk gewin, dat kan een voordeel zijn. Status zijn veel mensen ook heel gevoelig voor dat is een tweede. Een derde zijn mensen die wat meer gevoelig zijn voor interpersoonlijke relaties, dus wat anderen van hen vinden. Even als voorbeeld, volgens mij moet je goed gaan nadenken over de potentiele voordelen, nou carrière is er ook eentje, lijkt een beetje op status. Dus dat kunnen potentiele voordelen zijn voor een medewerker om wel of niet iets te doen. Als je kijkt naar nadelen, dan volgens mij is een van de belangrijkste nadelen dat mensen als ze zo iets al doen niet gezien willen worden, dat ze dat doen. Daar zit natuurlijk die deterrence theory achter. Daar zal je heel goed moeten nagaan hoe kun je mensen al de suggestie geven dat datgene wat zei doen snel zal worden opgemerkt en gezien zal worden. Dus dat betekend dat je op een hele goede zichtbare manier toezicht moet houden.
Even een zijstapje, wat een aantal jaren geleden bij NS is gebeurt, daar maakte ze altijd de stations schoon als er geen mensen op de perrons waren, want dat vonden ze altijd irritant en dan kun je gewoon lekker doorvegen en de mensen hebben er dan geen last van. Let maar eens op wat je tegenwoordig ziet, is dat dit gewoon op de drukste momenten gebeurt. Waarom? Omdat je ziet dat er wel echt wordt schoongemaakt en dat het gewoon een kerel is die je aan kunt spreken en die de moeite neemt om het hier allemaal schoon te vegen. Dus dat vergroot de drempel om op dat moment rotzooi te maken. Ook daar, misschien een tip voor je, ook om te gaan praten met de afdeling van de universiteit Groningen, die houdt zich bezig met allerlei experimenten op het gebied van toezicht, dus wat werkt nou wel wat werkt nou niet. Allerlei slimme experimenten, zei hebben bijvoorbeeld ook dat experiment gedaan dat ze keken in een steeg, daar hingen ze dan kaartjes aan fietsen en dan heb je

twee stegen, een steeg die helemaal goor was en een die heel mooi schoon was en ook lekker rook. En dan op het einde van de avond tellen hoeveel mensen hun kaartje op de grond hadden gegooid. Nou je kan wel raden: waar het vies is liggen veel meer kaartjes op de grond. Het schijnt zelfs ze te zijn dat wat het meest effect heeft, is dat als in een schone omgeving iemand in het zicht van alle andere heel duidelijk één kaartje op de grond gooit. Dat schijnt de grootste trigger te zijn om het gewenste gedrag te bevorderen. Dus je hebt eigenlijk iemand nodig die moedwillig de norm soms overtreed om te laten zien dat dát nou juist het afwijkende gedrag is. Die ene handeling zorgde er voor dat mensen zich veel netter gingen gedragen omdat het zo ver afstond van het [???]
Toezicht op een zichtbare manier, echt general deterrence. De suggestie geven dát. Ik geef ook vaak de suggestie, het blijkt te werken dat als je ergens een koffie apparaat neerzet en mensen moeten eerlijk betalen voor die koffie, dan is er geëxperimenteerd, we gaan die ruimte leuk maken met bloemen, mooie kleuren in de hoop dat mensen dat sympathiek vinden en dan gewoon eerlijk gaan betalen. Of we hangen er een poster neer, met ogen die heel indringend naar je kijken. Nou dat tweede dat heeft een enorm effect. Het hoeft niet eens echte controle te zijn, maar de suggestie van controle is al genoeg. Dus dat zou de organisatie ook al mee kunnen nemen hoe je dat op een slimme manier kan doen. Dat zal je wel constant moeten blijven vernieuwen want als je dat lang genoeg op dezelfde manier aanpakt dan is het uiteindelijk uitgewerkt. Dan treed er gewenning op.
Q: Beleid groeit vaak vanuit specifieke gebeurtenissen. Wat is volgens u een effectieve verdeling van aandacht op het gebied van algemene en specifieke cyber afweer?
Dat heeft volgens mij met de volwassenheid van de organisaties te maken. Want je ziet inderdaad dat organisaties die wat minder volwassen zijn op het gebied van risicobeheersing, dus ik trek hem even in het algemeen, die zullen pas maatregelen nemen naar aanleiding van incidenten. We hebben een incident, nu moeten we naar aanleiding van dit incident iets gaan doen en vaak stopt het dan ook. Want dan hebben we iets gedaan en dan denkt men dat het af is. Hoe hoger je dan op de volwassenheidsladder komt hoe meer een met risicobeheersingsbril er gekeken wordt naar hoe er zaken worden gedaan in de organisatie. Wat je gewenst zou willen, als dat je ambitie in ieder geval is, dus wat een hoog volwassenheidsniveau is, dat een organisatie die heeft een bepaalde missie, een visie. En in die missie en visie zal je ook al moeten nadenken op welke manier je aankijkt tegen het onderwerp criminaliteit en cyber risico's. Dat vraagt weer dat wij die missie kunnen waar maken door dit soort maatregelen maar vooral ook door deze cultuur in de organisatie te krijgen in plaats in plaats van dat je na elke gebeurtenis weer een nieuwe maatregel gaat krijgen, want even weer terug naar het voorbeeld van die incidenten bij die ziekenhuizen, dan kom je weer bij het stapelen van allerlei maatregelen, maar daar zit gewoon een maximum aan wat mensen aankunnen en wat effectief is. Hoe volwassener een organisatie is hoe meer ze gaan denken aan preventie in plaats van reactie. En ook 'hier staan wij voor en dat betekend dus', en hoe meer ze ook nadenken over cultuur en gedrag in plaats van allerlei harde maatregelen alleen.
Q: Adviseert u een cyber beleid aan de hand van een bepaalde standaard, of past u liever 'custom made' tactieken toe?
Je hebt natuurlijk allerlei cyber standaarden, daar ben ik niet in thuis, dus dat is denk ik wel even goed voor jou om te weten, nou ja waar ik altijd bij help is juist even terug naar cultuur & gedrag en dat dat de basis zou moeten zijn vanuit waar je als organisatie zou moeten willen opereren en daar hebben wij wel een cultuur model voor wat je zou kunnen gebruiken, dat heet het [[soft controls model]] waarin 8 cultuur elementen zitten en daarin ook inmiddels bewezen is wetenschappelijk dat naarmate die 8 cultuur elementen verder verankert zitten in de organisatie, dus meer volwassen zijn, hoe minder kans op incidenten. Dus die gebruiken we wel. Uiteindelijk is alles custom made omdat ik er gewoonweg niet in geloof dat je organisaties 1 op 1 met elkaar kunt vergelijken. Je zult altijd moeten nadenken van wat was bij deze organisatie de algemene cultuur, hoe werken mensen hier en wat past dan, gegeven dat, het beste. Dus wat slaat dan het beste aan. Ik kan je nog wel even de 8 elementen opsommen…
SBT (Social Bond Theory)
De theorie luidt dat zwakke sociale verhoudingen / banden aanleiding kunnen geven tot crimineel gedrag. De insider binnen een organisatie kan door weinig affiniteit met de zaak of een gebrek aan loyaliteit besluiten toe te slaan.
Q: Gelooft u dat werknemers een natuurlijke drang hebben naar crimineel gedrag die onderdrukt moet worden op een bepaalde manier?

Komen we terug naar die 5%, hetzelfde antwoord. Ik denk dat het niet zozeer de opzet is. Mensen hebben altijd een drang om te kiezen voor de makkelijke weg. Die drang zit er wel, dat maakt dat wij mensen zijn. Wij hebben ook altijd een drang om aardig gevonden te worden in de sociale omgeving waarin we ons bevinden. Groepsconformisme heet dat, dat zit heel erg in de mens. Als wij ons dus in een omgeving bevinden waarin crimineel gedrag of eigenlijk het gedrag dat de ongeschreven norm is, dan zijn we geneigd om daar mee te gaan.
[Q: wat denk je over mensen die zich expres buiten de groep willen zetten, die een aversie hebben voor groepsconformisme]
Dat kan op verschillende manieren. Je kan je ook buiten de groep zetten door op extreme manieren juist het gewenste gedrag te laten zien. Bij crimineel gedrag dan kom je weer bij allerlei criminologische theorieën. Volgens mij is bewezen dat opvoeding heel erg belangrijk is, nurture, en dus ook hoe ziet je familie eruit, kom je uit een sociaal zwak milieu ja of nee en dat dat veel meer belangrijke voorspellers zijn over de mate waarin je daar gevoelig voor bent dan anderen.
Q: Ziet u toepassing van, of een rol voor, informele controle (oftewel sociale banden, sociale controle) binnen een cyber security beleid?
Zeker. Dan zitten we weer bij dat social proof groepsconformisme. Kijk maar eens op youtube naar het ash experiment. Daar kan je je antwoord op vinden. [overeenstemmingsexperimenten van Asch: mening van mensen wordt bepaald door de meerderheid in een groep ; groepsconformisme] Dus je moet goed gaan nadenken over hoe de groepsnorm de gewenste norm gaat worden. En hoe kunnen groepen mensen elkaar op een gezonde manier scherp houden. Een van de voorbeelden die wij wel eens bij een klant hebben gebruikt is dat wij mystery guest activiteiten ontwikkelen waarmee de medewerkers zelf bij elkaar eigenlijk moesten checken of er wel op de juiste manier werd omgegaan met die mensen, dus op een soort challenge manier. Op een leuke manier dat sociale controle ontwikkeld.
Q: Hoe ziet u de mogelijkheid tot het beïnvloeden van de houding van werknemers tegenover niet-conform security gedrag?

SLT (Social Learning Theory)
Volgens deze theorie is crimineel gedrag aangeleerd of afgekeken. De insider kan beïnvloed worden door gedrag dat hij afkijkt van anderen, of gedrag dat door zijn collega's van hem verwacht wordt maar niet conform het security beleid is.
Q: Word er bij het opstellen van beleid rekening gehouden met eventueel aanleren, afkijken en imiteren van 'slecht' (lees onveilig) gedrag omtrent cyber?
Nou over het algemeen vind ik dat blijkt dat er veel te weinig wordt nagedacht over cultuur en gedrag. Dus wat is nou het gewenst gedrag dat we willen zien en wat is daar nou voor nodig. Moet je dan inderdaad in een sociale omgeving aanpakken om dat gewenste gedrag te creëren. Dus eigenlijk is deze vraag ook al deels beantwoord.
Q: Wat is volgens u de invloed van de bedrijfscultuur op haar werknemers en hoe belangrijk acht u die rol?
Heel groot. Culture eats strategy for breakfast.
TPB (Theory of Planned Behaviour)
De theorie stelt dat intentie voorafgaat aan daadwerkelijk gedrag richting misbruik of non – conform gedrag en daardoor een belangrijke rol speelt in het verklaren van gedrag. Houding en persoonlijke gedachten over bepaald gedrag kunnen de insider zowel motiveren als demotiveren bepaald gedrag te vertonen.
Q: Is er een huidige rol binnen security beleid om de intentie tot non – conform gedrag te beïnvloeden om cyber incidenten te voorkomen en hoe wordt dit aangepakt?
Dit is één element. Dus intentie en motivatie houding. Dat pak ik even onder dezelfde noemer. Maar ik denk juist dat dat juist nog veel meer word beïnvloed door de omgeving. Dus onze motivatie is dus eigenlijk een element, maar kijk vooral naar die sociale omgeving en die cultuur.
[Q: ligt er een rol bij de werkgever om ook te letten op die sociale omgeving en die cultuur?]
Nee dat lijkt me onuitvoerbaar om te doen. Je kan her hoogstens bij de screening en binnenkomst rekening mee houden. Tegelijkertijd geloof ik echt dat die beïnvloedsfeer in je bedrijf, in je pand veel groter is en zou je je veel meer daar op moeten focussen. Dus hopen dat het gedrag wat je wenst op de vloer ook mee naar buiten genomen wordt. Dus als mensen naar huis reizen of thuis werken op

dezelfde manier om gaan met informatie zoals ze dat in het pand doen.
Q: Hoe ziet u de rol tussen intentie en het daadwerkelijk uitvoeren van gedrag bij zowel accidentiele als opzettelijke incidenten?
Het is altijd heel moeilijk te bewijzen of iets opzettelijk is, omdat ik denk dat heel veel van ons gedrag ook wel min of meer dat wij gedwongen worden bepaald gedrag te vertonen en dat we dan achteraf zeggen dat dat expres was. Maar als dat evident is, dat iemand dat ook toegeeft dat het opzet was, dan is er volgens mij wel een 1 op 1 relatie tussen intentie en opzettelijk incident. Bij accidentele, ik denk dus dat de meeste incidenten per ongeluk gebeuren, omdat mensen niet scherp zijn, of niet door anderen worden geattendeerd op hun gedrag of teveel in de gelegenheid werden gesteld om dat te doen, dus min of meer verleid om bepaald gedrag te laten zien, 'omdat het nou eenmaal kon'. Dus als je de beschikking krijgt over bepaalde data of jij bent in staat om vanuit jouw rol bepaalde autorisatie toe te wijzen, nou grote kans dat je daarmee een keer de mist in gaat.
[Q: Doet mij een beetje denken aan de rational actor versus environment influence]
Ik denk dat dat altijd aan de gang is. Nu bijvoorbeeld ook, als ik heel kort zou antwoorden dan heeft dat ook een invloed op jou.
SCP (Theory of Situational Crime Prevention)
De theorie stelt dat criminaliteit niet alleen ontstaat wanneer er motief is, maar ook als de mogelijkheid zich hiervoor voordoet. Een insider die in eerste instantie geen plannen heeft een actie uit te voeren, kan overgehaald worden dit wel te doen als hij zich realiseert dat er een mogelijkheid voor is.
Q: Wordt er in cyber beleid rekening gehouden met condities die potentieel non security conform gedrag uit kunnen lokken ofwel kunnen hinderen?
Ja dat denk ik wel. Volgens mij denken organisaties juist na over wat nou de risico's zijn. Wie heeft er nou beschikking over welke data en wie heeft nou bepaalde authorisaties. Wie heeft er nou veel contact met de buitenwereld? Wie is er in staat bepaalde overschrijvingen te doen binnen de organisatie? Ik denk dat daar juist heel veel aandacht voor is, om vanuit daar te denken, en om daar allerlei maatregelen op te bedenken om dat zoveel mogelijk te beperken ik denk ook dat dat juist goed is. Het is wel de nadruk leggen op het negatieve. Terwijl je ook kunt nadenken over hoe we nou juist het gewenste gedrag kunnen bevorderen in plaats van het ongewenste gedrag minimaliseren, dat vind ik toch wel wat anders . Sancties tegenover belonen. Mensen zijn veel gevoeliger voor belonen dan voor straffen, dat is al bewezen. Dus mensen die passen hun gedrag eerder aan als ze gestimuleerd worden dan als ze worden afgestraft.
Q: Hebben de factoren: 'moeite, risico, beloning, provocatie en excuses' huidig een rol in security beleid?
Ik denk dus de eerste 4 wel, de laatste kan ik me minder wat bij voorstellen.
Q: Hoe word omgegaan met de factoren aansprakelijkheid en verantwoordelijkheid in een cyber security beleid?
Volgens mij kun je tegenwoordig wel zeggen dat uiteindelijk een CIO al aansprakelijk is als er echt iets mis gaat ook al heeft hij het niet zelf gedaan, maar hij wordt er wel op nagekeken. Maar de medewerkers hebben wel de verantwoordelijkheid om op een verantwoorde manier om te gaan met security.
Afsluitende vraag
Q: Naar uw mening, waar is de grootste inhaalslag op het gebied van cyber security momenteel te halen? Op welk gebied en op welke manier?
Ik denk dus wel investeren in cultuur en gedrag. Omdat ik zie dat security bij heel veel organisaties toch óf door een combinatie van security mensen wordt gedaan en techneuten dus IT achtige achtergronden en ik zie nauwelijks nog psychologen, nurtures, criminologen die zich met dit vak bezig houden en ik geloof dus dat gedragsbeïnvloeding echt veel meer effecten kan hebben dan allerlei technische maatregelen. Dat bijvoorbeeld op een afdeling security ook mensen komen te werken met een andere achtergrond, zoals sociologie of psychologie en die kennis dus ook gaan inbrengen en dat we vanuit daar ook beleid gaan doen.

Attachment 6 Original transcription of the fifth interview

Interview nr. 5 – Strategic advisor information security

Insider threat

Volgens de theorie en kijkend naar de grootste (en de meest kostige) incidenten is het gevaar van de eigen medewerkers van het bedrijf die cyber schade toe richten groten dan de dreiging van buitenaf.

Q: Kijkend naar dreigingen die de mogelijkheid hebben veel schade aan te richten, zijn interne of externe dreigingen het belangrijkste focus gebied volgens u en waarom?

Wat ik nu zie is dat vrij veel aandacht, hangt een beetje van het toepassingsgebied af, op externe dreigingen gezet of gekeken wordt. Maar dat hang heel erg van het domein af. Dat zit vrij veel in ontwikkelingen waar je echt externe actoren probeert het hoofd te bieden. Als dat dan de focus is dan is dan ook dat waar je uiteindelijk naar gaat kijken en maatregelen gaat nemen. Voor een deel zit daar denk ik ook nog steeds meer ontwikkeling in van de menselijke factor als dreiging of degene die het per ongeluk verstiert en ik denk dat het eigenlijk betreft de oorzaak niet zo veel uit zou mogen maken omdat je het wil hebben over welk effect je nu eigenlijk zou willen voorkomen. Dus ik zie nu dat zie je in dreiging analyse maar ook naar kwetsbaarheden zoeken, er word primair gekeken wat is nu eigenlijk de oorzaak en zijn er dingen die mis kunnen gaan en dan blijft in een aantal gevallen vrij impliciet van welk effect we nu eigenlijk proberen te voorkomen. En door het heel erg op te splitsen in deel gebiedjes word het ook best wel onduidelijk of je nou met zijn allen naar hetzelfde effect aan het werken bent of dat iedereen zijn eigen richting aan het bepalen is. Bijvoorbeeld, als het effect zou moeten zijn dat je werk op een veilige manier kan doen, dan kunnen maatregelen ook tegen je gaan werken als niet goed opgelet wordt dat het doel is dat je je werk veilig uit kunt voeren, in plaats van dat verteld word dat je veilig gedrag moet vertonen. Dus ik denk dat het vooral veel uitmaakt van de focus welke rol je ook hebt en welk doel gekeken wordt wat je nou probeert te bereiken. Nu zelf zitten we dus veel met externe dreigingen en de maatregelen daar tegen te verzinnen. Maar ik denk dat bijvoorbeeld banken daar heel anders naar kijken, ik denk dat het heel erg per sector ook verschilt als ik zo kijk. Het ligt aan wie er mee bezig is.

Q: Qua interne dreiging, hoe ziet u de verhoudingen tussen accidentiele (accidential) en opzettelijke (malicious) incidenten en hoe word hier met het opstellen van beleid rekening mee gehouden?

Wat ik nu zie is eigenlijk dat het als twee losse bronnen gezien wordt, dus ook weer van opzettelijk of niet opzettelijke incidenten. Ik denk dat ook daar veel verschil zit in hoe organisaties daar mee omgaan. Bijvoorbeeld bedrijven die meer vanuit de safety hoek komen die kijken niet zozeer naar de opzettelijke cyber incidenten omdat die meer uitgaan van een veiligheidssituatie waar mensen niet bewust de zaak zitten te verstieren. Maar ik denk dat nu, zeker vergeleken met hoe het was nu wel meer aandacht is standaard voor überhaupt wat kan er mis gaan en wat zijn de negatieve effecten maar ook wel steeds meer gekeken word met name uit vanuit [???] Jumbo effectus hoek [???] kun je nou mensen ook pinpointen die potentieel gedrag gaan vertonen die jouw organisatie gaan schaden. Dus ik denk dat zeker met het opstellen van beleid steeds meer naar de menselijke factor gekeken wordt. Waar ik nu wel een verschil zie is tussen awareness en daadwerkelijk het identificeren van potentieel negatief gedrag voor de organisatie. Dus ik kan nu wel tegen mensen vertellen dat ze niet teveel chocolade mogen eten, maar dat zegt niet dat ze het ook niet gaan doen.

Q: Hoe ziet u het verband tussen een werkbare werkomgeving en een veilige werkomgeving?

Ja wat ik zie is dat is volgens mij netto. Moet je op een veilige manier je werk uit kunnen voeren of moet je veilig werken. Als je je werk op een veilige manier uit moet kunnen voeren dan zet je de mensen die in het primaire proces zitten centraal, dus bijvoorbeeld ik moet een koekje van A naar B vervoeren, dat wil ik doen en dat wil ik op een veilige manier doen, dat is wat anders dan de security officer vertellen dat hij vanuit een bepaald perspectief deze maatregelen goed uit moet voeren. Dus als centraal staat van we hebben verzonnen dat er veilige maatregelen zijn en die moet je goed uitvoeren, dat is wat ik nu nog veel zie en eigenlijk waar je naar toe wil is een omgeving die kijkt naar wat je nou eigenlijk moet doen en hoe gaan we dat nou zo veilig mogelijk faciliteren. Dat is denk ik vooral wat ik hier zie met het verschil tussen een werkbare werkomgeving en een veilige werkomgeving ook omdat namelijk veilig een contrainerbegrip is. wat voor de één veilig is, is voor de ander zwaar problematisch. En dan kan ik een heel goed voorbeeld geven, de bewaking vindt dat de deur dicht moet blijven, maar als ik daar elke dag met een pakketje door heen moet is dat super irritant.

Security vs business wordt nu feitelijk tegenover elkaar gezet. Alsof het tegenstrijdig is en dat is ook het grote probleem denk ik van security op dit moment, dat security wel denken de business te ondersteunen, maar dat feitelijk niet doen. Bijvoorbeeld, stel je zit op een schip en vanuit security is bedacht dat het veilig is als je met een pasje in het security systeem in moet loggen. Dan kan niemand gaan zitten viespeuken en je weet wie wat gedaan heeft. Dat is super handig als je in de haven ligt en Jan en alleman aan boord kan lopen. Als je eenmaal op volle zee zit en je moet een reddingsmissie uitvoeren en Pietje valt met zijn hoofd op een bureau en er moet snel iemand bijkomen, dan wil je niet dat die eerst zijn pasje moet gaan zoeken om in dat systeem in te loggen. Dus wat je ziet is dat in omgevingen waar de context of de setting of het proces en wat je moet doen niet zo heel veel veranderd is dat niet zo problematisch, maar in een omgeving waar je af en toe andere dingen moet doen dan is aan de ene kant die maatregel helpvol en aan de andere kant houdt die je tegen. En dat zijn dus zaken waar veel te weinig naar gekeken wordt en zeker nu waar we in de maatschappij in omgevingen komen waar je feitelijk veel met dynamisch werk moet kunnen doen, met veranderende infrastructuren en een heel star regime van maatregelen en regels ie je allemaal na moet leven. En die regels zijn vaak activiteiten die uitgevoerd moeten worden en als je naar die activiteiten kijkt en zegt hoe dragen die nou bij met het veilig houden en maken van zaken, dan is de relatie vaak zoek. En dat soort, met name de maatregelen, er worden veel maatregelen bedacht omdat iemand zich ooit zorgen maakte en die heeft bedacht omdat hij zich zorgen maakte moet je inloggen met een pasje, maar dat is degene die zich vanuit security perspectief zorgen heeft gemaakt, en degene die het werk moet doen die zit met een heel ander probleem. Of die twee op elkaar passen, dat is de vraag. Als je mazzel hebt dan heb je goede security mensen die doen dat, maar vaak is de business praat niet in de taal van de security en de security is niet de taal van de business. Dan word er wel gezegd dat de gebruiker centraal staat, maar staat de gebruiker centraal dat je hem uit moet leggen hoe die security maatregelen moet treffen, of staat de gebruiker centraal omdat je hem gaat helpen zijn werk te doen. Voor de grap moet je maar eens luistern en die vraag je in je hoofd stellen en luisteren wat ze zeggen daar komen af en toe hele verrassende resultaten uit.

GDT (General Deterrence Theory)

Volgens de theorie is crimineel gedrag logischerwijs te verklaren aan de hand van het maximaliseren van voordelen en het minimaliseren van nadelen. Insiders binnen een organisatie kunnen handelen vanuit dit principe en slaan mogelijk toe wanneer zei bevinden dat een actie hen veel voordelen brengt.

Q: Als we kijken naar het maximaliseren van voordelen en het minimaliseren van nadelen voor potentiele cyber crime, waar kan dan volgens u op algemeen gebied rekening mee gehouden worden? De maatregel gedachten. Als ik het primair zou zeggen, op het algemene gebied wat zijn dan negatieve effecten die we niet willen dat die optreden en vervolgens dan gaan kijken waar kan je die effecten dan wel of niet zien. Dus je wilt bijvoorbeeld zo'n cybercrime, dat is iets wat jou negatief gaat raken. Wat is dan zo'n manier waarop jij negatief geraakt wordt en waar kan je dan aannemen dat dat aan het gebeuren is. Wat ik nu namelijk zie is dat best wel veel maatregelen verzonnen worden die dat moeten voorkomen, vervolgens wordt er gekeken naar hoe goed die maatregelen werken: de performance van de maatregelen maar in theorie in de hele security management cyclus wordt daar wel naar gekeken: hoe effectief is de maatregel dan, maar of die dan effectief is ten opzichte van het effect dat je wel of niet wil zien dat ontbreekt nog wel eens. Een concreet voorbeeld is dat heel lang geleden de Nederlandse overheid heeft bedacht dat we economisch worden geraakt door cybercrime, hoe komt cybercrime nou tot stand, dat wordt gefaciliteerd door botnets. Als je nou het aantal botnets omlaag brengt, dan neemt ook de cybercrime af. Dus wat gaan we doen? Zorgen dat er minder botnets komen. Wat hebben ze toen bedacht: we gaan de ISP's meer maatregelen uit laten voeren. Dat is 1) ze moeten een meldpunt hebben waar mensen kunnen melden dat er een bot in het netwerk van de ISP zit. 2) Ze moeten een quarantaine functie hebben dus die bot moet geïsoleerd kunnen worden. 3) Hij moet opgeschoond kunnen worden, dus feitelijk geneutraliseerd kunnen worden. Vervolgens gaan ze toetsen al die ISP's, werken die maatregelen wel goed? Dus je belt zo'n ISP op, wordt er binnen 10 seconden die telefoon opgenomen? Als de telefoon opgenomen wordt en je doet een melding wordt die bot dan in quarantaine gezet? Gebeurt ook, wordt dan daarna de bot ook opgeschoond? Dus als je dan die maatregel op die manier gaat beoordelen is de conclusie dat het aantal bots is afgenomen, dus de cybercrime is afgenomen. En toen heeft Michel van Eeten van de universiteit Delft onderzoek gedaan over hoeveel bots er nou gemiddeld bij die ISP's in een netwerk

zitten en dan krijg je een enorme spreiding. En wat er dus gebeurt is het effect dat je wil hebben is dat het aantal bots omlaag gaan, in plaats van dat er gemonitord wordt gaan die bots ook omlaag, wordt alle effort gestopt in het verzinnen en controleren van de maatregelen die uitgevoerd moeten worden. Dit is één voorbeeld en dit zie je in de praktijk best wel veel terug komen. Dus als ik zeg van algemeen: wat is nou als we kijken naar de vraag, dan zou ik vooral zeggen wat is nou het effect dat je wil voorkomen en ga daar op focussen, in plaats van dat je dan gaat zitten op afweer of preventie begint er mee van wat wil je nou überhaupt zien of niet zien.
Q: Beleid groeit vaak vanuit specifieke gebeurtenissen. Wat is volgens u een effectieve verdeling van aandacht op het gebied van algemene en specifieke cyber afweer?
Wat ik zie, is die algemene zaken, van wat is nou het effect dat we wel of niet willen zien, daar blijven focussen dat zie ik wel als een voordeel. Wat ik nou in die incidentgedreven aanpak veel zie, is wat ze noemen de risico – regel – reflex. Er gebeurt iets, daar ga ik maatregelen voor treffen en vervolgens ga ik heel erg zitten sturen of die maatregelen wel getroffen worden. Iets wat ik net in dat voorbeeld gaf. Het gevolg daarvan is dat men zich blind gaat staren op het werken van die maatregelen en vergeten te kijken naar of het gewenste effect nou wel of niet op treedt. Dus ook daar zou ik zeggen: de aandacht primair zou op het effect moeten zijn en daar moet je ook iedere keer op terugvallen om te checken of je nog steeds de goede dingen doet. Dat je de goede dingen doet geloof ik wel, maar in de veranderende omstandigheden nog steeds de goede dingen doen dat is wel een puntje van zorg.
[Q: ziet u vanuit de risico – regel – reflex dat er wel eens teveel gefocust word op incidenten die inmiddels verouderd zijn, maar dat er nog steeds erg op gehamerd wordt?]
Zeker, kijk maar bijvoorbeeld naar de gemiddelde Baseline. Waar bestaat dat ding uit, daar heeft iemand ooit een keer gezien dat iets mis kan gaan, die heeft een maatregel verzonnen en die komt in de Baseline te zitten en iedereen gaat die Baseline implementeren. Maar de vraag is welke problemen lossen we dan op? En by the way, als ik die maatregel niet invoer, wie vindt dat dan zorgelijk? Dat is in generieke termen best wel te benoemen, maar als je dat specifiek in organisaties gaat plotten is dat super ingewikkeld om die vraag beantwoord te krijgen. Dat komt ook meer van dat een iemand zal die maatregel super vinden omdat het voor hem zijn probleem oplost, maar voor een ander is het super irritant omdat het zijn werk belemmerd. Je kan dus beter over die effecten gaan sturen dan over de maatregel kant en over de incidenten voorkomen. Uiteindelijk netto komt het min of meer op hetzelfde neer, alleen ga je zo meer gefocust op de dingen die meer effectief zijn zitten. Dat is wel iets dat zijn van die hele subtiele verschillen en dat zie je vaak niet terug in de uitvoering van beleid, het hangt heel erg van de personen af die het dan uiteindelijk uitvoeren of ze dat verschil wel of niet zien, maar dat haal je niet uit je beleid of je strategie of de uitvoering over het algemeen.
Q: Adviseert u een cyber beleid aan de hand van een bepaalde standaard, of past u liever ‘custom made’ tactieken toe?
Ik denk dat die bepaalde standaarden heel goed voor inspiratie zijn, niet voor niks want heel veel mensen hebben er over nagedacht maar tune het dan wel op wat je nodig hebt. Van die standaarden dat zijn vaak dingen om iets goed te doen, maar dat wil niet zeggen dat je de goede dingen daarmee doet. Dat is een beetje hetzelfde als dat in de standaard staat dat je je pas moet gebruiken om in te loggen, maar dat is niet in alle gevallen slim om te doen. Dan kun je heel goed gaan zitten op hoe implementeer ik nou een pas systeem, dat kan je super goed doen, maar dat wil niet zeggen dat je het probleem op lost. Ik heb daar ook wel een filmpje van die heel goed laat zien dat je heel secure oplossingen hebt die het probleem niet oplost. Zie bijvoorbeeld het voorbeeld van het schip, waar het pasjes systeem versoepeld op zee. En dat je dan ook de taak van wie dan het besluit neemt op een andere plek neer legt dus ook degene die besluiten neemt ga je centraal stellen en wat het effect van zijn besluit is bij andere personen die andere doelen nastreven dus andere zorgen ook hebben. En dat spelletje wordt steeds ingewikkelder naarmate de organisaties ook groter worden.
SBT (Social Bond Theory)
De theorie luidt dat zwakke sociale verhoudingen / banden aanleiding kunnen geven tot crimineel gedrag. De insider binnen een organisatie kan door weinig affiniteit met de zaak of een gebrek aan loyaliteit besluiten toe te slaan.
Q: Gelooft u dat werknemers een natuurlijke drang hebben naar crimineel gedrag die onderdrukt moet worden op een bepaalde manier?
Nee. Volgens mij is dat ook laatst in een iets andere context hebben ze dat ook laten zien, door meer

fraude opsporing te doen en mensen aanspreken op potentieel frauduleus gedrag, dat dat juist fraude in de hand werkt. Volgens mij recent, de laatste twee weken kwam dat ook wat in het nieuws voor. Wat je nu ziet, de sociale dienst, die gaat steeds meer controleren op bijvoorbeeld uitkeringsfraude, maar het feit dat mensen daar op gecontroleerd worden of feitelijk gewoon al beschuldigd worden om dat te doen, werkt in de hand dat ze dat ook echt gaan doen. Als je toch al schuldig bevonden wordt, waarom zou je dan nog moeite doen om het niet te doen? Dus ik denk dat als het hier ook over gaat denk ik niet dat werknemers een natuurlijke drang hebben naar crimineel gedrag maar dat feitelijk een 'giftige (toxic) omgeving', zo zal ik het maar even noemen, van je organisatie dat wel in de hand kan werken. Deels zal dat in individuen zitten die dat gedrag überhaupt gaan vertonen, maar dat kan wel versterkt worden als je een giftige organisatie hebt die feitelijk meer individuen in die richting gaan duwen. En dat zou je dan kunnen verwoorden als een verziekte bedrijfscultuur en dat kan bijvoorbeeld zijn door of dat kun je in de hand werken met iedereen te controleren of ze wel doen wat afgesproken is dus het hangt ook van het type organisatie af. Maar als je in een professionele organisatie zit en je gaat iedere keer aan mensen vragen of ze alles wel netjes hebben gedaan, dan werk je in de hand dat mensen zich af gaan vragen waarom ze het überhaupt nog doen.
Stel er is er één die jat in een organisatie, en vervolgens maak je iedereen schuldig of je geeft een signaal af dat iedereen niet vertrouwd wordt, dan krijg je die sociale hechtingen, dus jullie vertrouwen mij niet, wat is mijn loyaliteit dan terug? En dat werkt gedrag in de hand wat je feitelijk niet wil.
Q: Ziet u toepassing van, of een rol voor, informele controle (oftewel sociale banden, sociale controle) binnen een cyber security beleid?
Ja, sociale controle zou ik het niet per se willen noemen, maar ik zou wel bijvoorbeeld als je mensen een rol wil geven in veiligheid van je organisatie, wat dat ook is, dan zou ik ze vooral maatregelen geven die kopieer gedrag in de hand werken. Er is een theorie van een collega in Groningen, die heeft ooit een model ontwikkeld waarbij je succes van diensten kan voorspellen. Een van de elementen erin is hoe makkelijk mensen dat kunnen kopiëren. Dat had hij van spelende kinderen. Waarom leren kinderen spelen? Een kind ziet een ander kind met een bal spelen en die gaat dat kopiëren en dan gaan ze vervolgens spelen. Wat je naar mijn idee van als je niet de sociale controle, maar juist de sociale banden versterkt door maatregelen die mensen uit kunnen voeren, maar door te laten zien hoe je dat doet, andere mensen dat gedrag ook over gaan nemen. Dus eigenlijk kopieer je een uitvoerbaar gedrag. Dat zie je in concrete vorm als je zegt dat het hele bedrijf pasjes zichtbaar moet dragen omdat je ook wel wil dat mensen een ander kunnen aanspreken op dat ze dat zichtbaar doen om mensen die kunnen binnen sluipen weg te houden, maakt het nogal uit wie dat laat zien en of mensen dat ook gaan kopiëren. Als gezegd word vanuit het management dat je dat moet doen, maar het management doet het niet, dus die laten gedrag zien wat je niet wil en mensen gaan dat kopiëren omdat ze zeggen dat als dat toch niet gebeurt, dan ga ik dat gedrag kopiëren. Je wilt juist positief gedrag kopieerbaar maken, maar ook laten zien dat je dat doet. Er is ook de vraag van kun je dan ook een cultuur creëren dat mensen elkaar ook aan gaan spreken als ze dat niet doen en dat werkt heel slecht in een bedrijf waar een angstcultuur heerst. Als je het niet doet en je krijgt direct op je flikken, dat gaat ook niet erg goed werken.
Q: Hoe ziet u de mogelijkheid tot het beïnvloeden van de houding van werknemers tegenover niet-conform security gedrag?
Ja. Persoonlijk heb ik toch altijd wel wat moeite met niet conform zijn, want dat werkt heel erg in de hand dat het om compliance zou moeten gaan. En als je het toch hebt over het mogelijk beïnvloeden van de houding van werknemers, dan ook daar weer gaat het om welke effecten wil je zien en ze daar op aanspreken, niet of ze nou een maatregel wel of niet nageleefd hebben. Misschien hebben ze vanuit hun expertise, dat zie je vaak vanuit de praktijk, iets veel slimmers verzonnen om dat effect voor elkaar te krijgen. En gewoon de simpelste test om dat te doen zijn dingen als stiptheidacties. Wat is dat, dat is het strikt naleven van de regels en wat gebeurt er dan, dan stort het hele proces in. Dat betekent ook dat we vanuit compliance en de security organisatie graag fantaseren dat wat we voorschrijven dat dat gebeurt en dat daarmee de risico's weg zijn. Als vervolgens mensen dat ook heel strikt gaan doen dan werkt er helemaal niks meer. Dus je kunt beter ook daar weer sturen op wat is het effect dat je wilt zien en niet op niet – conformiteit gaan sturen maar meer op of het effect dat we niet willen zien al aan het optreden is of niet.
[Q: ziet u een manier waarom de inbreng van die expertise gereguleerd kan worden?]
Ik denk dat het nu, in de breedte een beetje aan de opleidingen skillset ligt mist om dat goed te doen.

Wat er nu veel gedaan wordt in die opleidingen, is dat je allerlei security maatregelen hebt en security management zorgt ervoor dat die maatregelen netjes worden uitgevoerd. In feite compliance. Maar als je niet expliciet in die opleiding feitelijk aangeleerd krijgt om de vraag te stellen hoe de organisatie dat gaat helpen, dan ga je nooit op die effecten focussen, effectiviteit als wat je wel of niet wilt zien. Bijvoorbeeld net als met die bots, als je bij een ISP werkt zeg je: we willen gewoon minder bots hebben. Dat is het effect dat je wilt zien en wij denken dat je daar een quarantaine functie moet hebben die goed werkt en een opschoon functie die goed werkt. Als iemand anders een idee heeft om het effect op een andere manier te bereiken, dan wil je dat ook graag boven tafel hebben en de mensen die daar zitten hebben echt wel verstand van zaken over hoe ze dat moeten doen. Wat er dan vaak gebeurt is dat de maatregelen op een hoger dek worden verzonnen, op een niveau waar men niet zo goed weet hoe dat werkt of niet de expertise hebben om dat goed te doen en dat wordt vervolgens naar beneden gedrukt dat dat zo gedaan moet worden en dan zou het allemaal wel goed komen. Dus bijvoorbeeld wordt een afdelingsmanager gevraagd of hij al die maatregelen wel netjes uit heeft gevoerd, dan zegt hij ja ik heb al deze activiteiten gedaan en vervolgens heeft hij al die activiteiten ingevuld dus kan hij dat allemaal mooi afvinken als activiteiten, maar die bots zijn er nog steeds. Dus ook als je daar niet op gaat sturen dan word het A) vinken exercitie en B) het draagt niet bij aan het beter veiliger maken of effectiever zijn van die organisatie. En dat is ook een beetje een menselijk aspect een human factor dingetje, hoe je dat zou kunnen of moeten doen.
Waar het vooral over gaat en dat krijg je natuurlijk ook nooit helemaal weg gemanaged, je kan vaak een hoop werk besparen door minder te focussen op het uitvoeren van activiteiten en veel meer op de resultaten en effecten die je daaruit wil zien. Als je dat eenmaal ziet dan is dat bloed irritant, want dan zie je het overal oppoppen. En het is vooral die dingen eruit vissen die gewoon daadwerkelijk ook heel veel tijd kosten en niet tot een specifiek resultaat of bepaald effect leiden. We hebben een hoop voorbeelden gehad, dat kan heel simpel zijn, bijvoorbeeld de rapportage structuur of de rapportage lijn veranderen. Vaak gaat de analyse van incidenten en de security organisatie is via bepaalde functionele hiërarchie ingericht en dat is ook hoe dingen organiseren en de rapportage lijnen inrichten en nu zie je vaak dat door de top de doelen van het bedrijf worden gesteld, dat dat via die hiërarchie naar beneden druppelt en dat onder iedereen naar de doelen van de organisatie richt, prima als je met die blik kijkt en je gaat via die manier inrichten is het een heel logisch verhaal, als je dan op al die punten in de functionele hark gaat kijken hoe er gewerkt wordt, dan kom je altijd vrij vaak in een netwerk structuur terecht:' ik doe wat en dat is voor die organisatie onderdeel ik lever wat op en dat is voor dat organisatie deel en om dat te kunnen doen ben ik afhankelijk van die partij en die zit binnen en die zit buiten'. Dus op al die knooppunten zie je dat al die doelen op een andere manier geïnterpreteerd en ingevuld worden maar de rapportage loopt via die hiërarchie. Dat betekend ook dat als je een probleem of eigenlijk iets wilt veranderen door informatie die je hebt wel te rapporteren, maar dat komt alleen in de hiërarchie en niet op de plek waar je er wat mee kunt, het enige wat je dan hoeft te doen is zeggen ik kan dus dingen veranderen door het in de goede rapportagelijn te gooien, namelijk in de manier waarop wij werken en daar op gaan sturen en niet blind staren op hoe die functionele hark in elkaar zit. Dan moet je eens met bestuur gaan praten, die hebben daar onwijs veel moeite mee en zeker ook hoe nu risico managers, bestuurders, management in het algemeen opgeleid worden is werken vanuit een functionele hiërarchie en iedereen werkt aan de doelen van de organisatie. Dan kijk je daar naar en dan kun je dat wel heel hard denken, heel hard willen en heel hard geloven, maar misschien is de realiteit wel even anders.
SLT (Social Learning Theory)
Volgens deze theorie is crimineel gedrag aangeleerd of afgekeken. De insider kan beïnvloed worden door gedrag dat hij afkijkt van anderen, of gedrag dat door zijn collega's van hem verwacht wordt maar niet conform het security beleid is.
Q: Word er bij het opstellen van beleid rekening gehouden met eventueel aanleren, afkijken en imiteren van 'slecht' (lees onveilig) gedrag omtrent cyber?
Volgens mij niet. Ook wat ik net zei, hoe kun je dat nou bevorderen? Door maatregelen te kopiëren die kopieerbaar zijn. Er wordt vrij veel gekeken naar welke maatregelen vanuit een security perspectief goed zijn, maar er word helemaal niet gekeken naar hoe je kunt stimuleren dat mensen makkelijk dat gedrag kopiëren. En sommige maatregelen zijn niet kopieerbaar, maar dat gaan we via awareness sessies proberen uit te leggen. Waar ook wel weinig rekening mee gehouden wordt is dat 'onveilig' een containerbegrip geworden is. En dat voor de een veilig echt wat anders betekend dan

voor de ander. Hoe ik het zeg, van wat is nou veilig, dat is dat je je werk gewoon goed uit kunt voeren, whatever that may be. En onveilig is dat dat dan niet kan. En dan is het dus afhankelijk van met wie je praat en wat zijn werk is wat dan wel of niet veilig is. Bijvoorbeeld er ooit een analyse gedaan in de [???] keten, sociale werk en inkomen, een partij die eindverantwoordelijk is voor de informatie wisseling tussen de sociale verzekeringsbank de gemeentes en dat soort zaken, heel erg zit te drukken op het naleven van privacy regels, want dat is voor die hele keten goed en dat moet ook. Maar hoe harder er in die keten gedrukt word op privacy maatregelen, het werk voor de gemeente steeds moeilijker word. Waarom? Omdat privacy op die manier vertaald [betaald??] is van je hebt op dat moment een bakje nodig om een bepaald type werk te doen, en alleen als je dat type werk doet mag je in het bakje graaien: lees ik mag iets voor werk en inkomen doen. Maar als die gegevens in dat bakje nou de beste zijn die ik heb en ik mag dat ook gebruiken voor het bestrijden van jeugdwerkeloosheid of sociale cohesie in de buurt, dan krijg ik binnen de gemeente die een taakstelling heeft met minder werk met minder mensen beter werk moet gaan leveren wat ga je dan doen? Dan ga je in dat bakje graaien. Dan zie je dus dat de ene kant gedrukt wordt van dat je alleen in dat bakje mag graaien als je dat werk zit te doen en aan de andere kant zit heel erg de neiging om werk goed te willen doen, dus ik moet in dat bakje graaien. Dan zie je voor de ene partij het risico afnemen, want er word minder in een bakje gegraaid als dat niet nodig is, aan de andere kant ontstaat een probleem want die kan zijn werk niet meer goed doen. Dan is de vraag of harder drukken op het uitoefenen van die maatregelen gaat dat dan effectief zijn? Ik denk het niet. Dat is ook wel een beetje in dit verhaal, waarom doe je het, het is veilig en als je met twee partijen aan tafel zit hebben ze dan ook hetzelfde beeld van wat veilig is en hebben ze dat ook getoetst?

Q: Wat is volgens u de invloed van de bedrijfscultuur op haar werknemers en hoe belangrijk acht u die rol?

Bedrijfscultuur is super belangrijk. Als de bedrijfscultuur is dat je eigenlijk vanuit de top uit impliciet of expliciet je medewerkers niet vertrouwt of niet gebruik maakt van de kracht die ze inherent hebben, dat gaat geheid negatieve effecten opleveren. Angstcultuur, dat mensen dingen verzwijgen die je eigenlijk wel wilt weten. Wantrouwen in je medewerkers gaat leiden tot gedrag dat je niet wilt hebben. Dus ja dat kan een enorme impact hebben. Je kan een hele giftige bedrijfscultuur hebben. ***<u>En daar word trouwens vrij weinig onderzoek naar gedaan, dat is mijn beeld.</u>*** Dus er wordt wel heel veel onderzoek gedaan naar wanneer mensen nou crimineel gedrag gaan vertonen, ook intern, maar er is heel weinig onderzoek naar wat nou die toxische effecten zijn die die cultuur in de hand werken.

TPB (Theory of Planned Behaviour)

De theorie stelt dat intentie voorafgaat aan daadwerkelijk gedrag richting misbruik of non – conform gedrag en daardoor een belangrijke rol speelt in het verklaren van gedrag. Houding en persoonlijke gedachten over bepaald gedrag kunnen de insider zowel motiveren als demotiveren bepaald gedrag te vertonen.

Q: Is er een huidige rol binnen security beleid om de intentie tot non – conform gedrag te beïnvloeden om cyber incidenten te voorkomen en hoe wordt dit aangepakt?

Ik zie dat daar steeds meer aandacht voor komt. Het is ook een beetje opkomend, er zijn niet zo heel veel partijen die hier concreet mee bezig zijn. Ik zie bijvoorbeeld sign post six, die is daar heel druk mee bezig. Die doen met name dit. Je ziet dat het niet standaard is, het is ook redelijk nieuw, maar dat is wel een belangrijk aspect om daar ook wel effectief mee te zijn. Het is wel redelijk beperkt wat je hier op ziet, tenminste wat ik zie. Hoe meet je intentie, hoe ga je dat waarnemen en organiseren? Dat is niet dat het dan direct moeilijk is, maar ook hoe allerlei mensen dat een organisatie dat dan moet gaan doen, dat is wel een bottleneck. Het idee is niet zo lastig, maar hoe krijg je het geïmplementeerd?

Q: Hoe ziet u de rol tussen intentie en het daadwerkelijk uitvoeren van gedrag bij zowel accidentiele als opzettelijke incidenten?

Het verschil tussen genialiteit en stupiditeit is dat er een grens zit aan genialiteit. Dus die accidentiele dingen die blijven we toch wel houden. Opzettelijk incidenten zit ook deels in vrij vaak stapeling van rechten noem ik het maar even. Grote incidenten, ook in de bankaire wereld hoe kan dat nou? Mensen zijn van functie naar functie naar functie gegaan en hebben al die rechten van al die functies mee gekregen, vervolgens konden ze dingen doen die eigenlijk niet mochten. Dus deels is het de opportunity wordt ook mede geschapen doordat een aantal dingen in het security beleid niet op orde zijn.

SCP (Theory of Situational Crime Prevention)
De theorie stelt dat criminaliteit niet alleen ontstaat wanneer er motief is, maar ook als de mogelijkheid zich hiervoor voordoet. Een insider die in eerste instantie geen plannen heeft een actie uit te voeren, kan overgehaald worden dit wel te doen als hij zich realiseert dat er een mogelijkheid voor is.
Q: Wordt er in cyber beleid rekening gehouden met condities die potentieel non security conform gedrag uit kunnen lokken ofwel kunnen hinderen?
Wat ik zie is dat gebeurt op verschillende manieren. Dus eentje die ik net zei: mensen gaan rechten stapelen tijdens het wisselen van functies terwijl in het beleid staat dat dat ingetrokken moet worden en om allerlei redenen gebeurt dat niet. Een ander voorbeeld is dat je ziet dat in een bedrijfsproces separation of duty wordt gedaan, dus segregation of duty. Dus bijvoorbeeld in een betaalproces zet een iemand de rekening klaar iemand anders controleert en dan wordt ie pas betaald door een derde persoon. Dat hebben ze dan netjes ontworpen, dan ga je aan de onderkant kijken hoe dat in het IT systeem geregeld is en dan zit daar één administrator onder. Dus soms is het ook niet intentioneel maar er worden gewoon dingen over het hoofd gezien. De vertaling van de business requirements dus naar de IT systemen dan bijvoorbeeld. Dan is het business proces helemaal dicht getimmerd, en dan begint de opportunity in de technologie te komen. En dan creëer je daar onbewust dus een potentieel risico. Het is nogal apart dat je aan de ene kant de moeite neemt om 3 man erop te zetten en aan de andere kant maar 1 man aan de knopjes die ook alles kan doen. Beleid zou dan voor moeten schrijven dat je dat netjes gescheiden hebt maar dan is dat toch ergens mis gegaan in de hoogte. En dan creëer je dus onbewust ook al is het in het beleid netjes omschreven hoe je dat moet doen dan door die afstemming creëer je allemaal gaten waar mensen misbruik van kunnen maken.
Je ziet vooral in de organisatie die moet de business IT lijn heel erg op orde hebben wil je dit soort zaken spotten. Maar het feit dat we door ICT incidenten heel veel organisaties in crisis komen is ook al een indicatie dat hun business IT lijn niet helemaal oké is. Daar is een hele simpele test voor, dat heet black swans & perfect storms. Als er een IT incident is geweest en de organisatie is in een crisis gekomen, dat zou alleen maar kunnen door incidenten waarvan je van te voren niet kon voorspellen dat ze eraan zaten te komen → black swan of in gevallen dat een opeenstapeling van allerlei factoren leidt tot incidenten → perfect storm alles wat daar tussen in zit dan ben je gewoon niet op de hoogte met je risico management.
Q: Hebben de factoren: 'moeite, risico, beloning, provocatie en excuses' huidig een rol in security beleid?
Nee ik denk dat dat al wel langer speelt als het gaat over social engineering dat zijn volgens mij wel wat factoren waar daar naar gekeken wordt. Of het echt strak in het security beleid netjes geïmplementeerd word dat je daar ook effectief tegen bent dat weet ik niet. Ik denk dat dat ook wel een interessante vraag is van wat voor data kun je nou vinden wat de schade is van insider threats. Of dat nou afneemt, toeneemt, of dat bepaalde sectoren harder geraakt worden dan andere en of er dan een relatie heeft met het beleid dat ze daarop hebben geschreven. Ik denk dat die informatie gewoon niet boven de tafel te krijgen is.
Dat is interessant om te kijken of het beleid iets voorschrijft om iets te voorkomen of niet. Voer een activiteit niet uit, maar je moet je werk wel doen. Een voorbeeld is in de automitive hoek. Daar stond een artikel van een lease maatschappij en die had kastjes in de auto zitten en op een begeven moment stond heel die vloot van de lease maatschappij stil. Waren allemaal remote disabled. Het eerste artikel ging over dat een hacker de gehele vloot had gedisabled. Ging je verder zoeken, kwam er een verhaal uit dat het een insider was, die was ontslagen en die had de credentials nog. Dan ging dus dat artikel van hacker naar "omar was goed met IT en had de wachtwoorden nog". Dus sommige dingen worden insider threats hacken genoemd, maar het is gewoon geen zicht vanuit management wat iemand doet en kan en vervolgens bij het uit dienst gaan niet nadenken over wat je allemaal uit handen af kan nemen. Wel de sleutels van de voordeur, maar niet de credentials. Hoe denk je dan dat dat vaak mis kan gaan? Wat vaak hacker gebeuren word genoemd, is vaak mensen hebben gewoon toegang tot een systeem en die worden op een of andere manier gemotiveerd om iets te doen.
Q: Hoe word omgegaan met de factoren aansprakelijkheid en verantwoordelijkheid in een cyber security beleid?
Dat zijn termen van wil je daar nou in je beleid mee schermen. Aansprakelijkheid weet ik niet, zit voor een deel, heb ik met defensie ook mee gemaakt, met staatsgeheimen als je daar niet aan voldoet

ben je ook persoonlijk aansprakelijk dus in sommige gevallen kan ik me er wel iets bij voorstellen. Verantwoordelijkheid is ook wel een hele leuke, want wat wij nu doen aan analyse is kijken naar je hebt een bepaald poppetje die heeft bepaalde doelen en zijn belangen zijn het realiseren van die doelen. Niet kunnen realiseren van die primaire doelen is een risico dat hij loopt. En wat je dan ziet is dat poppetjes verantwoordelijk gemaakt worden voor iets en als je dan gaat kijken naar wat zijn nou de doelen waar naar dat poppetje moet streven en hoe komt dat overeen met de verantwoordelijkheid die hem toebedeelt is, daar zitten vaak al gaten en kleine gaatjes tussen. Dat betekend ook dat als je niet nadenkt over het beleggen van verantwoordelijkheden of in welke mate die in lijn zijn met de doelen die dat organisatie onderdeel of dat poppetje moet nastreven dan is er al een gat in je security beleid ontstaan of creëer je in feite daarmee een risico. En wat dan vanuit het beleid bedacht is: we hebben de verantwoordelijkheid belegt dus dat is op orde, en doordat je niet de check doet maar is het in lijn met wat dat poppetje überhaupt moet doen, ja het is feitelijk een inherent risico dat je gecreëerd hebt, terwijl het eigenlijk bedoelt was om het risico te voorkomen. Dat klinkt een beetje paradoxaal, maar dat gebeurt vrij veel.
[Als iemand de verantwoordelijkheid heeft om iets voor elkaar te krijgen, maar de verantwoordelijkheid niet krijgt, hoe gaat hij het dan voor elkaar krijgen?] Ja precies.
Ik kan nog wel een concreet voorbeeld geven, een paar jaar geleden in het nationaal cyber security strategie nog een discussie. Er zat iemand in de overheid, van CZ en iemand van een middelgrote ISP zaten onder andere aan tafelen de overheid zei: jullie moeten de verantwoordelijkheid voor cyber security risico's en die ISP zegt: maar wij hebben onze risico's op orde en ik zit daar zo een beetje bij te luisteren in die discussie of die risico's wel of niet goed op worden genomen. De overheid vond dat ze meer verantwoordelijkheid moesten nemen, ISP zegt we hebben onze verantwoordelijkheid allemaal goed geregeld, en dan is mijn vraag, maar wat zijn die risico's waar jullie het over hebben? De overheid heeft het over maatschappelijke risico's, de ISP over bedrijfsrisico's. Dan zeg ik: misschien is dat niet helemaal hetzelfde. En ook daar zie je weer, dat als je in hele generieke termen over verantwoordelijkheid en risico's blijft praten, dat het helemaal niet duidelijk is of die nou wel of niet op elkaar matchen. Je moet ze meer specificeren.

Afsluitende vraag

Q: Naar uw mening, waar is de grootste inhaalslag op het gebied van cyber security momenteel te halen? Op welk gebied en op welke manier?
Veel meer vanuit de partijen die betrokken zijn redeneren wat is nou, wanneer gaat het in jouw optiek goed of niet. Dus wanneer die doelen wanneer ga je die nou wel of niet halen. En het wel of niet halen van die specifieke doelen dat zijn de risico's waar je over moet praten. En om die doelen te kunnen halen ben je afhankelijk van anderen en wat we nu veel doen is praten over wat er in die afhankelijkheid mis kan gaan. Bijvoorbeeld, iemand levert diensten niet, dan denk ik so what, als hij die diensten niet levert dan kan ik ze ergens anders vandaan halen dan is er nog steeds geen probleem. Bijvoorbeeld, stel nou ik ga een feestje organiseren en ik denk er komen een man of 10. En ik stuur een uitnodiging uit en ik heb intussen naar de supermarkt gegaan en voor 10 man eten en drinken gehaald, een klein barretje en wat muziek en ruimte in mijn eigen huiskamer. Dan loopt het een beetje uit de hand want een of andere sukkel zet een open uitnodiging op facebook en dan komt er 100.000 man. Het doel was: ik ga een feestje organiseren voor 10 man en ik heb de afhankelijkheid van de catering en de ruimte enzo op orde. Nou komen er 100.000 man is dat nou een probleem? Dat is een probleem als ik niet een feestje van 100.000 man kan organiseren dus bijvoorbeeld de afhankelijkheden ik kan onvoldoende drank in slaan want ik heb de financiële middelen even niet beschikbaar als ik dat allemaal op orde kan brengen, dan ben ik nog steeds succesvol, namelijk ik haal het doel om een leuk feestje te organiseren. En dat is denk ik waar risico management over zou gaan: is van, ook bij veranderende doelen en van afhankelijkheden, kan ik dan nog steeds succesvol zijn. En wat we nu doen: we hebben bedacht wat er mis kan gaan, we hebben maatregelen getroffen, en we gaan heel erg nadenken of die maatregelen goed uitgevoerd zijn. Of we dat doel succesvol halen? Geen clue. Sterker nog, dat gaan we allemaal niet dynamisch vast stellen. Ondertussen zijn de afhankelijkheden dynamisch, de doelen dynamisch, de manier waarop je samenwerkt om het doel te realiseren is dynamisch geworden en dan zitten we ondertussen lekker statisch die risico management volgens compliance regels na te leven.
[dus jij zou liever in de richting gaan waar we het doel in zicht houden en ons niet zo vast pinnen op de maatregelen die we nemen om dat veilig te doen?]

Sterker nog, om te beseffen dat het doel van de een niet het doel van de ander is en daarmee het risico van de een never het risico van de ander kan zijn. Dat besef alleen al, dat je niet met 12 man aan tafel over de risico's van die 12 man kan hebben, dat is al enorme winst. En als je het al over risico's hebt dat je dan zeker kan zeggen die groepen gaan steeds groter worden dus steeds meer stakeholds bij waar je moet gaan analyseren en wat die gaan doen is steeds meer dingen op tafel leggen die mis kunnen gaan. Of dat erg is, van al die partijen, dat komt pas op het einde een keer, als je mazzel hebt, naar voren. Om dat een beetje te stroomlijnen kunnen we veel meer nadenken of we het kunnen relateren aan het doel en voor wie dan, kun je ook bepalen moet ik het hier überhaupt over hebben, zitten de goede partijen wel aan tafel of is het helemaal niet relevant? En met name met meerdere stakeholders sneller de relevantie van wat besproken wordt van tafel kunnen vegen wordt steeds belangrijker.
[ziet u ook een manier waarop we dat beter kunnen gaan doen?]
De methodes hebben we, die hebben we ook met een aantal mensen ontwikkeld bij [Redacted] waar het grootste probleem zit is om mensen in een andere denkmodus te krijgen. Dus wat ik net zei, dus van blijven mensen nou denken en geloven in de functionele hark en organisatie zijn ze ook in staat om de switch te maken af en toe te denken en te kijken naar de manier waarop gewerkt wordt. En kunnen ze ook dat op een manier organiseren waarop security en risico management kunnen ze dan dat op elkaar gaan knopen. En wat we zien is we hebben twee analogieën. De een is wat minder handig om dat nogal een geloofskwestie is, geloof je nou of de aarde het middelpunt van het universum is of de zon. Er veranderd niks maar als je op een andere manier kijkt worden dingen wel simpeler verklaarbaar. En de andere is van een organisatie gedraagt zich via twee modellen net als licht: je hebt een golf en een deeltje: functionele hark en je hebt een manier van werken. Je moet even weten wanneer je met welk model je aan de slag moet om dingen op orde te krijgen. Wat we zien is dat die twee modellen moet je eigenlijk continue op elkaar blijven plakken dus als je naar techniek kijkt kun je naar techniek kijken, maar als je daar je organisatie model niet bovenop legt dan heb je een hele secure oplossing maar dan heb je bijvoorbeeld, dat heb ik in de praktijk gezien, dan heb je een hele secure oplossing met allerlei technologie waar allemaal geheime sleutels in verwerkt zijn, en langzamerhand is die organisatie een beetje veranderd en is die management ge outsourced. Een ding wat je niet moet doen is als je verantwoordelijk bent voor de veiligheid van jouw infrastructuur de sleutels daarvoor bij een externe partij neerleggen. En dat klinkt super logisch, dat dat niet slim is, maar als je alleen vanuit de techniek perspectief kijkt en je niet dan de organisatie kant erop plakt, dan zie je dat niet eens. En zeker wat wij nu zien is dat die organisatie uit steeds meer verschillende poppetjes gaan ontstaan die allerlei tegenstrijdige belangenverstrengelingen gaat hebben en dan ga je gewoon onwijs veel missen.
[dus daar moet iemand tussen komen die van alle afdelingen de belangen kan overzien?]
Ja, of je gaat mensen opleiden om te zien of ze hun doel en belangen en requirements wat scherper kunnen maken.
[dus ze meer integreren in de andere onderdelen van de organisatie]
Ja en dat is dus lastig want bijvoorbeeld wat heel moeilijk is, is om resultaten goed van tevoren te kunnen specificeren wanneer je nou blij bent met een bepaald resultaat. Om een voorbeeld te geven, als ik nou jou deze tekst geef en ik er zou een typefout in staan of een tekstuele fout dan kun je die er uit halen. Als ik nou jou vraag om te specificeren op de criteria waarop je die verbeteringen doorvoert, das dan hele lastige taal want dat ga je niet specificeren. Wat gebeurt er nou steeds meer, mensen die eigenlijk de expertise niet hebben om die specificaties op te stellen (lees mensen die een bedrijfsproces uitvoeren) gaan we vragen om dat soort specificaties namelijk specificaties voor een IT systeem op te leveren. En de mensen die het wel kunnen die IT specialisten thuis spreken de taal van de business niet nou wat krijg je dan, een heel duur systeem dat niet doet wat die gebruikers willen. Waar ligt dat dan aan? Ligt dat aan die IT'er? Ligt dat aan de business? Ligt het aan het gebrek hoe je dat vertaalt? Het is voor IT dat, maar het geldt voor steeds meer maatschappelijke processen. En het wordt allemaal zo specialistisch, dat het heel moeilijk is om van te voren te vertellen wat het nou is dat je precies van iemand wilt. Wat gebeurt er dan? Die iemand vraagt jou een activiteit uit te voeren, daar komt iets uit en dan krijg je dat in handen en kun je zeggen 'ja maar wacht even, dit moet even verbeterd worden'. En da vraag is heb je dan die tijd die je hebt gebruikt om elke keer die activiteit uit te laten voeren om dat te gaan verbeteren zodat je scherp hebt wat het resultaat wel moet zijn en ga je ondertussen die transitie in of blijf je ze maar vertellen wat mensen allemaal voor activiteit uit

moeten voeren? Dit is wat we de hele tijd aan het doen zijn. Omdat namelijk die vertaalslag we niet kunnen maken weet je, dat kost expertise, tijd, skills die we niet hebben, we hebben niet het besef dat je op een andere manier van kijken ook efficiënter kan worden van waar je moet focusen. Nou ja weet je dat gaan we voorlopig nog niet oplossen misschien ook wel leuk, we hebben voorlopig nog genoeg werk, maar af en toe denk je dat het wel een tikje sneller een tikje efficiënter en wat makkelijker en beter kunnen.
En ik denk dat de grootste slag is, het besef van het verschil tussen ben je nou mensen aan het helpen om hun werk te doen of ben je mensen aan het uitleggen of ben je de security aan het helpen zijn werk beter uitgevoerd te krijgen? Dat is denk ik, die vraag, die stellen en daarmee een stukje besef creëren wat doet dat security beleid nou eigenlijk? En vaak is dat security beleid gericht op zorgen die weet ik veel wie zich maken en dat uit gaan leggen aan de rest van de organisatie.